An Analysis of the Influence of Cultural Backgrounds of Individuals upon their Perspective towards Privacy within Internet Activities

Jehad Faisal Al Amri

Centre for Computer and Social Responsibility

The Faculty Technology

De Montfort University

Leicester

Submitted in partial fulfilment of the requirements for the

De Montfort University

Degree of Doctor of Philosophy

June 2012

DECLARATION

I hereby declare that this thesis is my own work and effort and that it has not been submitted anywhere for any award. Where other sources of information have been used, they have been acknowledged

ACKNOWLEDGEMENTS

I would like to thanks Taif University for funding my PhD study, Dr. N Ben Fairweather, Dr. Richard Howley and Dr. Sara Wilford for their cooperative supervision, valuable contribution, and helpful suggestions toward my thesis. Also I would like to extend my thanks to my parents (Faisal and Salwa) and my wife (Deena) for their supporting and to my daughters (Lma, Lamees and Lubna) for been in my life.

ABSTRACT

Concern about privacy is an important consideration for users of information and communication technologies (ICT), particularly when using computer-mediated communication (CMC), i.e. Internet usage. Several researchers have studied privacy issues by taking into account the views of users to include individuals, organisations, privacy policy makers, governments and trust organisations.

This thesis investigates whether an individual's perspectives about privacy are culturally relevant when using the Internet. This research used a survey in the form of a questionnaire in two countries, namely, Saudi Arabia and Malaysia to compare online privacy perspectives of young and mature (male and female) Saudi and Malaysian students. The research examines the relationship of the effect of the cultural background including the effect of social norms, religious belief, Internet regulation and IT skills of these Internet users upon their attitude towards privacy online and their perspectives about privacy. It also examines the effect of nationality (Malaysian and Saudi), gender and age groups. In this study, online privacy perspectives are a synthesis of three perceptions; what is 'personal' information online, the online privacy concerns and the Internet trust, whereby the cultural effects are the effect of religious beliefs, social norms, Internet regulation and IT skills in the privacy attitudes of keeping personal information safe, caring about their and others' privacy online and when revealing personal information. The demographic factors in this research are nationality, gender and age. To study these relationships, the research uses t-test, ANOVA, and single regression methods as data analysis techniques.

The results show that the level of concern and degree of trust exhibited by Malaysian students with regard to submitting personal information via the Internet was affected the most by their gender, and social norms upon their online privacy attitudes. For Saudi students, the level of concern and trust with regard to submitting personal information via the Internet was found to be related to the effect of their age, gender, and religious beliefs on their online privacy attitudes. The other cultural factors, i.e. Internet regulation in force in each country and the IT skills of participants, are likely to have equal effects on both Malaysian and Saudi privacy perspectives.

This research adds the cultural background, age and gender effects to the model of the calculus of the privacy concern that is proposed by Dinev and Hart (2006, pp. 63-64). The research also establishes what is 'private' in Malaysia and Saudi Arabia, by identifying "what counts as personal information with regard to Internet users" and provides a comparison in this concept between the two countries, their gender and age groups. For examples, Malaysian students consider name, e-mail address, date of birth, nationality and religion as 'personal' information and Saudi students consider home address, phone number, photographic image and credit card number as 'personal' information. In addition Saudi females tend to consider, particularly, home address, phone number, and photographic image as 'personal' information more than Saudi males.
These findings should help both web designers and Internet policy makers in Saudi Arabia and Malaysia to consider these cultural effects when designing the privacy policies of their websites.

KEY WORDS

Online privacy concerns, religious beliefs, social norms, Internet regulation and IT skills, Malaysia, Saudi Arabia, gender and age

USED ACRONYMS / ABBREVIATIONS[1]

ICT: Information and communication technology

CMC: Computer-mediated communication

PP: Privacy perspective

PI: Personal information

PC1: The Internet user's concerns about submitting personal information online

PC2: The Internet user's concerns about the possible unexpected, unauthorised or improper secondary use of the submitted personal information

IT1: The Internet user's concerns about handling personal information online

IT2: The Internet user's trust about the safety of the exchange personal information

SN: The effects of social norms on online privacy attitudes

RB: The effects of religious beliefs on online privacy attitudes

IR: The effects of Internet regulation on online privacy attitudes

ITS: The effects of IT skills on online privacy attitudes

KPI: Keeping personal information

CATPO: Caring about their privacy online

CAOPO: Caring about others' online privacy

CWRPI: Careful when revealing personal information

ANOVA: Analysis of Variance

[1] Another copy of this abbreviations' list is provided separately.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

1.1 INTRODUCTION

In today's world, more and more people are becoming familiar and competent in using a variety of technologies. With the advent of the 21st century, the question has become one of who controls these technologies rather than who actually owns them. This has raised the matter of who will control and regulate these technologies in the future. For this reason, issues and problems associated with computer ethics have become an essential part of the computer revolution (Moor 2001, pp.89-91). Privacy issues are wide ranging. They may involve an individual's right (Volkman 2003, p.199), a personal value, a claim or a form of control (Moor 2002, p.252). Privacy, therefore, is one of the most important issues associated with computer ethics. Thus, correspondingly, someone might be interested in privacy in order to guard their information, maintain their autonomy, protect their identity or control access to their person (Elgesem 2004, pp.418-435, Tavani and Moor 2004, pp.436-449 and Stahl 2008, pp.51-52).

Researchers argue that documentation that dates back to ancient Greece and China together with sources from Judaism, Christianity and Islam show us that alongside other values, such as, freedom of speech, privacy is a component of human dignity. It is a fundamental human right comparable with life, liberty and property. Privacy is protected in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights and it is respected around the world by different countries and cultures (PHR, 2005 - Overview of Privacy).

One key definition of privacy is "the right to be let alone" (Warren and Brandeis, 1980; Yang, 1966; Grant *et al*., 1988; Stahl, 2004). Nevertheless, the growth of technology has extended the meaning of privacy to include, specifically, the right to informational self-determination (Stahl, 2004). Consequently, in seeking privacy we might ask others not to enter our property, not to read our mail, not to know or retrieve our past, and so on, without our permission (Weckert, 1997).

According to Bellman *et al.* (2004), privacy concerns differ culturally and geographically. Kemp and Moore (2007), assert that privacy interests are culturally relative because a serious privacy violation committed in one culture may be acceptable by another. Much of the research into online behaviour identifies privacy as one of the most important issues for online users; therefore, the level of people's privacy concerns can affect their online behaviour (Dinev and Hart, 2006). The main aim, therefore, of my investigation is to discover whether there is a relationship between online privacy perspectives and an individual's cultural background. Such information could supply regulators with additional tools for improving privacy policies.

This chapter reviews the research carried out upon the area of interest, that is, online privacy. This is followed by an explanation of the research's aims, questions and its significance. Finally, the chapter concludes with an outline of the thesis so that the reader is able to gain a sense of the structure of the research.

1.2 ONLINE PRIVACY

The types of Internet activities that are undertaken link to the level of privacy concerns (Westin, 2001 and Dinev and Hart, 2003, p.6) and to Internet trust (Siala *et al.*, 2004, pp.8-9). Privacy concerns may be affected by the nature of information required for particular Internet activities (Dinev and Hart 2003, p.6 and Dinev and Hart 2006, p.31), the way that the information is collected and characteristics of the information collector, for example, e-commerce, e-government and social networks (Smith *et al.* 1996, p.189). With regard to Internet trust, which is the level of confidence among Internet users with regard to how their personal information will be used (Dinev and Hart, 2006, p.66), it indicates any uncertainty in the relationship with information providers that could affect a user's motivation to engage in online activities (Siala *et al.* 2004, pp.8-9, Dinev and Hart 2006, p.9).

A number of researchers (Chan *et al.* 2002, p.139, Ballman *et al.* 2004, p. 313, and Xu *et al.* 2008, p.7) claim that social norms, which could be defined as the collection of rules that are agreed and shared by members of a group within a social sphere (Cialdini and Trost, 1998, pp. 151-192), could affect (directly and indirectly) the extent of people's Internet activities by influencing their privacy concerns and trust in the Internet (Ballman *et al.* 2004, p.315, and Xu *et al.* 2008, p.7). Moreover for the members of the society, who could be partners, family, friends, colleagues and the media, social norms act as a social, rather than a force of law, to form the members' behaviours. Additionally these social norms which direct such social groups and their activities come from behaviours that are conducted and rewarded, and become the desired

reactions to circumstances within the society (Cialdini and Trost, 1998, pp. 151-192, and Amin and Ramayah, 2010, p. 3).

Other researchers identify a link between internet and computer use on the one hand and religious beliefs on the other. For example, the Islamic religion, (Zakaria *et al.* 2003, p.57, Siala *et al.* 2004, p.10, Barzilai-Nahon *et al*, 2005, pp. 25-40, Campbell, 2007, pp. 103-1062, Kluver and Cheong, 2007, pp. 1122- 1142 and Al-A'ali 2008, p.29). For example, a number of researchers (Zakaria *et al.* 2003, p.57, Siala *et al.* 2004, p.10. and Al-A'ali 2008, p.29) have studied the relationship between ethical issues including privacy and technology from the perspective of Islam. These researchers argue that Muslim countries tend to follow Islamic principles in their computer codes of conduct (Al-A'ali 2008, p.29). They also studied the concept of authority and its role in Internet usage, and the related ethical issues, for example, religious authority and how religious leaders and policy decisions affect the interpretation of official religious teaching and therefore threaten these authorities. Moreover the problem of authority within the Internet usage exists, given that some authority is challenged by Internet users (Campbell, 2007, pp. 103-1062). In addition, some researchers argue that in some conservative religions, the relation between IT and religion seems to be rather conflict ridden, for example the Internet is looked at as a modern phenomenon that has difficulty blending with the religious traditions (Barzilai-Nahon *et al*, 2005, pp. 25-40, and Kluver and Cheong, 2007, pp. 1122- 1142). Nevertheless, there is a paucity of studies into the effect of religion beliefs, particularly within the Islamic religion, and the online privacy perspective. In addition there is a lack of studies on the effects of social norms on the online privacy perspective of Internet users in Islamic countries therefore there is a need

for studies into the perspectives of individual Muslims with regard to the relationship between privacy and Internet usages.

Other researchers have investigated the effect of Internet regulation on the privacy concerns online (Milberg *et al.* 2000, pp. 35-57, Bellman *et al.* 2004, p.315 and Wirtz *et al.* 2006, pp.340-341). Internet regulation includes those created by both governments and corporations. The role of corporations, however, appears to be one of reacting to government regulations (Milberg *et al.* 2000, p 41). It has been argued that the relationship between privacy concerns of Internet users and their perception of Internet regulation is not just limited to the government regulation, but rather, extends to include the perception of the corporation management practice of the applying the Internet regulation proposed by the government (Milberg *et al.* 2000, p 42). This could be called the perception of private rules of the Internet regulation (Peek, 2007, pp. 165-166).

Other researchers have studied the relationship between the privacy concern of the Internet users and their IT skills (Tavani and Moor 2004, pp.436-449, Bellman *et al.* 2004, p.316 Moores, 2005, pp.86-91, and Dinev and Hart 2006, p.9). IT skills, which are considered as part of the organization culture (Stahl and Elbeltagi, 2004, p.48), could include knowledge about the range of information gathering techniques while they are online (Clarke 1999 p.60; Kelly and Rowland 2000, p.4) and knowledge of the technology and practices that could be facilitated to protect their privacy online (Tavani and Moor 2004, pp.436-449, and Moores, 2005, pp.86-91).

In addition, some studies have examined the relationship of Internet privacy concerns with gender (Slovic *et al.*, 1997 and Kehoe *et al.*, 1997, Bartel-Sheehan, 1999and Garbarino and Strabilevitz 2004, p.770,) and age (Liebermann and Stashevsky 2002, pp.297-298).

1.3 RESEARCH MOTIVATION AND AIMS

The motivation of this research is to develop a theoretical explanation for the social phenomena of individual Muslims' perspectives with regard to the relationship between privacy and Internet usage. This study sets out to investigate the relationship between privacy and the Internet and the affect upon it of the cultural backgrounds of individuals in Islamic cultures. To achieve this, two main aims need to be addressed:

(1) Identify the cultural influences that affect the privacy perspectives of individual Muslims with regard to their own Internet usage.

(2) Identify the similarities and differences between the perspectives of individual Muslims of different cultural backgrounds, namely, Saudi and Malaysian, with regard to the issue of privacy within ICT, i.e. Internet usage.

1.4 RESEARCH QUESTIONS

To explore these areas of study, the following questions need to be answered:

1) Is there a relationship between the level of an individual's concern over Internet privacy and the effects of their religious beliefs, IT skills, social norms and local Internet regulation?

2) Is there a relationship between the level of an individual's trust in the Internet and the effects of religious beliefs, IT skills, social norms and local Internet regulation?
3) How do individuals' religious beliefs, IT skills, social norms and local Internet regulations affect Internet privacy concerns and Internet trust?
4) What similarities and differences exist between Muslims from different cultural backgrounds, with regard to the effects of their religious beliefs, IT skills, social norms and local Internet regulation on both their Internet privacy concerns and their Internet trust?

1.5 THE SIGNIFICANCE OF THE RESEARCH

It is generally agreed that there is a common cultural understanding regarding privacy, because it is commonly accepted that it is a desirable and necessary right (Newell 1998, p.366). The effect, however, of cultural background and gender on individuals' perspectives towards privacy in Internet usage needs to be examined, particularly at the level of attitude, as certain acts may be interpreted as a violation of privacy in some cultures while not in others. The aim of this investigation is to explore the relationship between online privacy perspectives and Internet users' cultural backgrounds through their social norms, religious beliefs, the Internet regulations in their country, their IT skills, nationality and gender as mentioned in this introduction. This approach would supply Internet privacy regulators with additional tools with regard to online privacy so that cultural sensitivity of privacy policies could be addressed.

1.6 THE THESIS STRUCTURE

In order to accomplish the research's aims and questions as described in Sections 1.3 and 1.4, the thesis is divided into nine chapters (see Figure 1.1). Following this introductory chapter, Chapter Two contains the literature review, which discusses the research topic, that is, online privacy perspectives. The research methodology is described and discussed in Chapter Three. Chapter Four analyses the focus group, which acts as a pilot study for the research. Chapter Five discusses the research's design. In Chapter Six, the preliminary descriptive data analysis is presented. Chapter Seven details and discusses the inferences drawn from the data analysis. Finally, the discussion regarding the findings, recommendations and conclusions is summarized in Chapters Eight and Nine. There now follows a more detailed outline of the contents of each chapter:

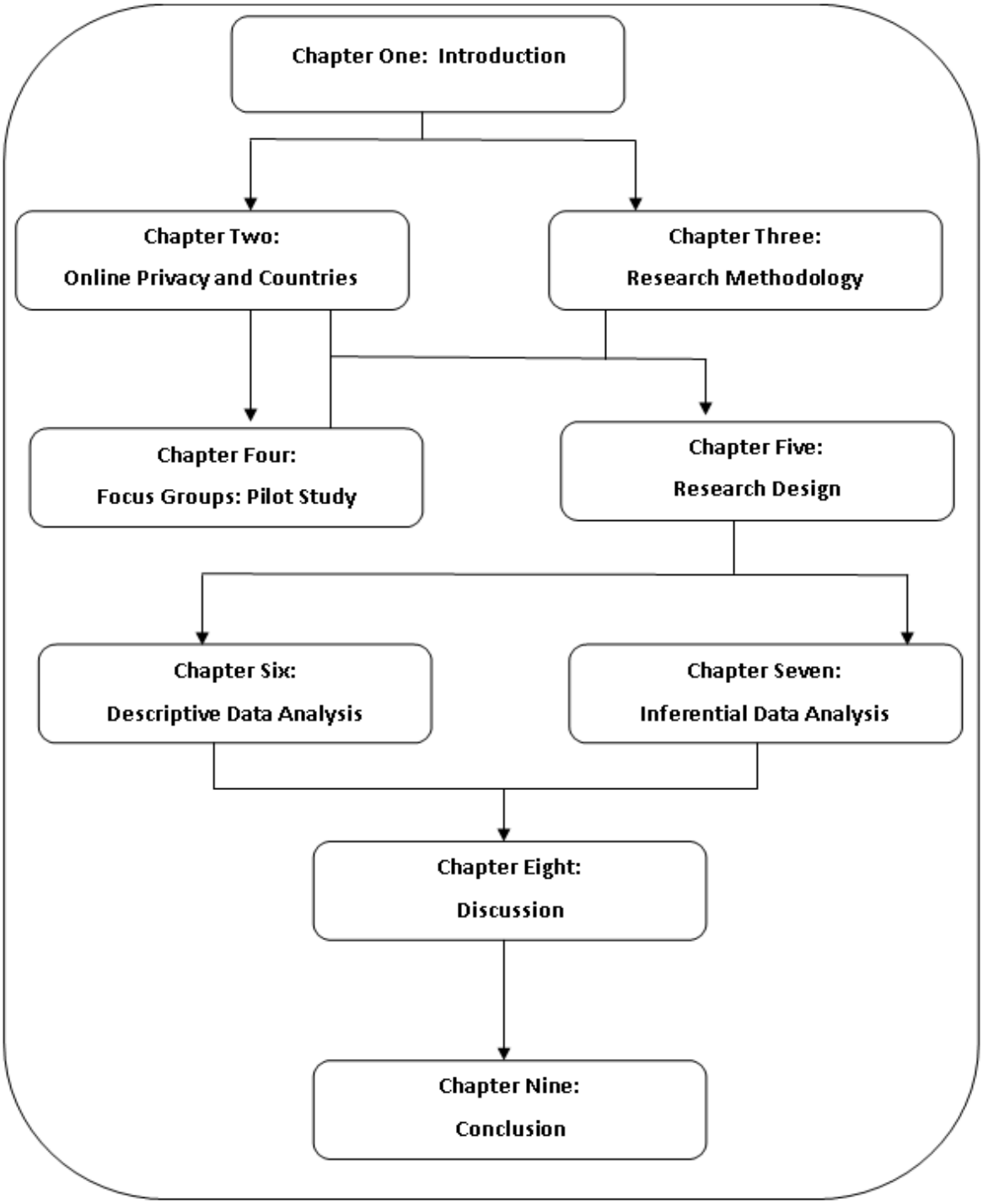


Figure 1-1: The Thesis Structure

- Chapter Two reviews online privacy as the area of investigation and national contexts as a background review of the countries to which the target participants belong. The online privacy perspectives cover the definitions of privacy concept, the main factors involved in measuring informational privacy, theories of privacy and the relationship between privacy, information communication technology (ICT) and culture. The country contexts cover general information about each one (Saudi Arabia and Malaysia) including their location, population and political system

- Chapter Three provides a review of research methodologies for information systems research. The chapter describes the ontological and epistemological considerations that relate to the research including the three main philosophical paradigms: the positivist, interpretive and critical paradigms. It also discusses both quantitative and qualitative research strategies, including research methods and data collection techniques, such as, interviews, questionnaires, case studies, focus groups and the intended research paradigm, methodology, methods of data collection and analysis strategies and techniques for this study.

- Chapter Four compares focus groups, surveys and individual interviews as data collection techniques. Issues associated with using focus groups as a social research method, including standardization, sampling, group size and numbers of groups and the use of focus groups as a social research strategy are discussed. Finally an analysis of the main outcomes of the focus groups is presented.

- Chapter Five describes the research design, including that of the questionnaire, its validation and translation processes and the structure of the data collection from both Saudi Arabia and Malaysia.

- Chapter Six provides full details of the data analysis, including the screening of the collected data with regard to outliers, normality, the reliability and validity of the questionnaires. In addition, details of an analysis into the demographic characteristics of the participants from Saudi Arabia and Malaysia and their Internet usage and activities; their level of online privacy concerns and trust; the effect on their attitude to the online privacy of family and friends; of religious beliefs; of Internet regulation and of IT skills are discussed.

- Chapter Seven relates the analysis of the effect of nationality, gender and age factors on participants' online privacy concerns and trust together their overall attitude toward online privacy. It looks at the outcomes of the test of the proposed research hypotheses using simple linear regression analyses.

- Chapter Eight presents a discussion of the results, particularly the effects of nationality, gender and age factors on online privacy concerns and trust and the online privacy attitude in the light of the literature review. This chapter also provides a summary on the cultural influences that affect the privacy perspectives of individual Saudi and Malaysian Muslims on their internet usage and identifies similarities and differences between their perspectives.

- Chapter Nine answers to the research questions, followed by a discussion of the research's limitations and directions for future research and a final conclusion

Next, is chapter two; it is designed to provide a literature review on online privacy as the area of investigation, particularly to study the concept of the privacy, its theories, measuring factors and relationship with Information Communication Technology (ICT). This chapter, also, discusses the characteristics of the desirable sample population of this research with a background on the selected countries, as the source of this sample population.

2 CHAPTER 2: ONLINE PRIVACY AND COUNTRIES CONTEXT

2.1 INTRODUCTION

In chapter one, the introduction to this thesis was provided including a number of preface points that include, first, the introduction to online privacy as the area of interest in this research, secondly, the research's aims, questions and its significance, and thirdly, the outline of the thesis. Now we will move to the literature review on online privacy as the area of investigation, and of research into the countries where fieldwork will take place.

Issues and problems associated with computer ethics have become an integral part of the computer revolution (Moor 2001, pp.89-91). Privacy is considered one of the issues that exert a significant influence over users' decisions when they engage in online activities (Dinev and Hart 2006, p.29). For example, online communications are much broader in scope, speed and nature than before and with Web 2.0 technologies, many more people now have the opportunity to gather, collate and disseminate information about others very easily on a global scale. The development of laws to deal with all these new capacities is much slower process than the development of the digital technology. Thus, privacy laws and policies have been slow to catch up with these new technologies (Lipton 2010, p.479). Moor (1985) describes the period between launching new technologies and producing associated policies as "policy vacuums" in the regulation of such technology. One of this research's aims is to investigate whether the privacy perspectives of individuals are associated with the privacy laws of each country in this investigation.

Research into online privacy perspectives highlights a number of factors that could affect such viewpoints, for example, age, gender, level of education, ethnic origin and social norms (Newall, 1998; Bellman *et al*, 2004,; Siala *et al*, 2004; and Xu *et al*, 2008). As discussed in chapter one, the aim of this research is to explore the relationship between online privacy perspectives and Internet users' cultural backgrounds, including their social norms, religious beliefs, their culture's Internet regulations, their IT skills, nationality and gender. In order to accomplish this, this research targets participants from two sample populations of two Islamic countries, namely, Saudi Arabia and Malaysia. The participants are Muslim students or members of staff at selected public universities from Saudi Arabia and Malaysia.

Divided into two parts, this chapter discusses online privacy and the context of the two countries. In the first part, online privacy, the concept of the privacy including the main factors involved in measuring informational privacy, privacy theories and its relationship with Information Communication Technology (ICT) and culture are reviewed. This is followed by a discussion on online privacy perspectives including the role and the nature of online personal information, the online information-provider and information-collector. In the second part, the country context, a background review of the countries from which the target participants are drawn i.e. Saudi Arabia and Malaysia is undertaken. This review will include their location, population, political system, their Internet services and privacy regulation. The higher education systems in each country are briefly described to provide background information about the sample population used by this research.

2.2 THE CONCEPT OF PRIVACY: THE PHILOSOPHY OF PRIVACY

Privacy is a concept that has been dramatically extended as it developed over time and it has become even more elastic in the contemporary computer age, particularly with regard to the latter's 'power stage', wherein threats to privacy can arise through identity disclosure and the ability to observe and link personal data (Senicar *et al.* 2003, p.148). While privacy has been recognized as a concept since the time of the ancient Greeks (Stahl 2004, p.63), it has since been re-defined in several ways. Judge Cooley, an American judge, who defined privacy as 'the right to be let alone', shaped one of those redefinitions (Warren and Brandeis 1890, p.195). More recently, the meaning of privacy has been extended to include, specifically, the right to informational self-determination, therefore, by seeking privacy, we might ask others not to enter our property, not to read our mail, not to know or retrieve our past and so on without our permission (Stahl 2004, p.63).

Furthermore, structuring a consistent definition of privacy in ordinary language is difficult and very challenging (Kemp and Moore 2007, p.58; Tavani, 2007, p.1). It has been argued that one of the reasons for this difficulty is that privacy is considered a rather non-static concept that consists of dynamic components, such as, political, technical and social features (Tavani 2008, p.132). Another reason for the difficulty is that people's interests in privacy vary; they might include controlling personal information, controlling access to one's location and person, obtaining autonomy, maintaining one's personal development and preserving a level of secrecy. Privacy interests are culturally relative and even if a particular action against privacy might be considered a serious violation of privacy in one culture, the same action might

nevertheless be considered perfectly acceptable in another culture (Kemp and Moore 2007, p.58). In subsection (2.2.1), the changing definitions of the privacy concept with time and the main factors involved in measuring informational privacy is summarised.

The aim of developing privacy theories is to provide a background for developing law and policies. According to Lipton (2010), most scholars consider one of three aspects of privacy when they try to form a privacy theory, for example, some of them focus on the nature of privacy rights, others attempt to categorize privacy-threatening conduct while, others are concerned about practical legal reforms that might provide better online privacy protection. This section will briefly discuss the justification for privacy according to the concepts of rights and value as ethical parameters, together with a summary of the three theories of privacy.

2.2.1 PRIVACY DEFINITIONS

Historically the definition of privacy is summarised as follows. Westin (1969) defined privacy as, "The claim to determine when, how and to what extent information about someone is communicated to others." (Margulis 2011, pp.10-11). In other words, privacy is a personal process of control whereby people have the means to choose between their desire for confidentiality or disclosure according to their situation and its social norms and their awareness of the possible costs of using that control (Spiekermann and Cranor 2009, p.68).

The need for privacy, according to Westin, works in tandem with other needs in maintaining people's emotional ability to engage with other people in daily life

(Margulis 2011, pp.10-11). Miller (1971) emphasised the importance of the ability to control the flow of personal information in order for the individual to attain the effective right to their privacy (Brandimarte, et al. 2010, p.4). Altman (1975) characterises privacy as, "The selective control of the access to the self." (from Margulis, 2011, p.11). In other words, there seems to be a process that regulates privacy that enables people to optimize their "openness" and "closeness" according to their circumstances (Spiekermann and Cranor 2009, p.68).

It is, however, worth mentioning that Westin and Altman's privacy definitions were formed prior to the pervasiveness of electronic environments (Spiekermann and Cranor 2009, p.68). The use of the Internet and online communication is associated with a number of complications with regard to the meaning of privacy. One of these complications is the assumption by the Internet users that online activities (similar to offline) could be private is misplaced. This is due to the mechanical nature of the Internet, which renders online conversations insecure compared to face-to-face or even telephone conversations (Walther, 2011, p.3).

In addition, Fried (1984) defines privacy as, "Not simply an absence of information about us in the minds of others, rather it is the control we have over information about ourselves." (Brandimarte, et al. 2010, p.4). For his part, Elgesem (1996) believes that "To have personal privacy is to have the ability to consent to the dissemination of personal information." (Brandimarte, *et al.* 2010, p.4). Furthermore, Stone *et al.* (1983), define privacy as, "The ability of the individual to personally control information about one's self." (cited in Smith *et al.*, 1996, p.189). Clarke (1999) defines informational

privacy, “As being a combination of personal communication privacy and personal data privacy.” (cited in Skinner, *et al*, 2005, p.981).

In addition, Clark (2006) classified the interpretation of privacy into four meanings. First is privacy of the person, which is more connected with the ‘human body’. Second is personal behaviour, which could be referred to as ‘media privacy’ and is related to sensitive matters, such as, the habits, religious and political views and activities of an individual. Third is personal communications, which could be referred to as ‘interception privacy’, where individuals seek the freedom to communicate privately among themselves. Fourth is personal data, which could be referred to as ‘information privacy’, where individuals seek the freedom to have a substantial degree of control over their data. According to Lessig (2001), privacy, similarly to copyright, is a way of controlling information. He said, “Just as the individual concerned about privacy wants to control who gets access to what and when, the copyright holder wants to control who gets access to what and when”.

Finally, Vasalou *et al.* (2011, pp.13-14) proposed eight high-level dictionary categories for privacy. These categories are:

- negative privacy (i.e. privacy concerns and risk related words)
- norms requisites (i.e. norms and beliefs relating to required privacy)
- outcome states (e.g. freedom, separation and being alone)
- private secrets (i.e. words stating the content of privacy, such as, secrets and data)
- intimacy (e.g. trust, friendship and confiding)

- law (e.g. policy, offence and confidentiality)
- restriction (e.g. lock and exclude)
- open visibility (e.g. posting, display and accessibility)

In summary, privacy's importance derives from different perspectives (see figure 2.1), which can be philosophical, psychological, sociological, economical and political (Clarke 2006, pp.1-2; Kemp and Moore 2007, pp.58-77). With regard to the philosophical perspective, it is very important for its own sake. It derives from the concepts of human dignity and the perception of individual autonomy and self-determination. The psychological perspective, comes from the principle that people need a private space from which they are able to judge the possible threats around them and decide how they going to act and what information to give about themselves. In terms of the sociological perspective, people need to be free to behave and associate with others as they wish without the threat of being observed. Concerning the economic perspective, people need to be free to innovate and from the risk of a lack of private space in which to exercise their innovation. Finally, with regard to the political perspective, people need to be free to think, argue and act within a relatively private space without the threat of being observed.

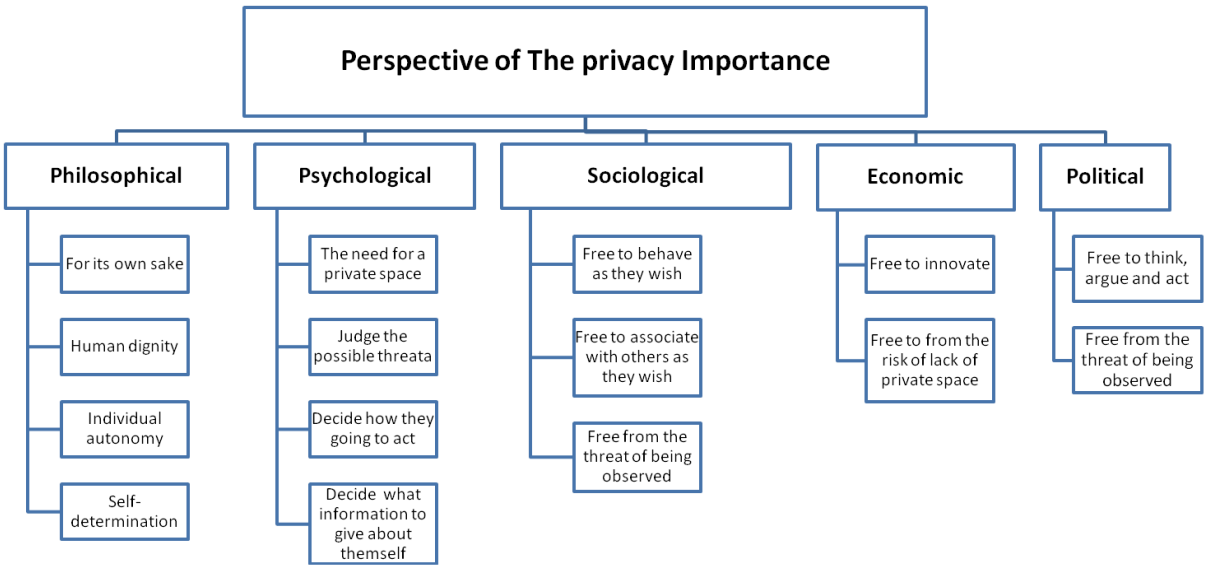


Figure 2-1: Perspectives of the Privacy Importance

2.2.2 FACTORS IN MEASURING INFORMATION PRIVACY

Lee and Kwon (2010, p.5194) classify the factors involved in measuring informational privacy concerns into six (see figure 2.2), all of which could be raised within one of the four stages of information handling, that is, input, process, output and storage. The first three factors, context data collection, tracking and recording, sensor and infrastructure could be identified and measured at the input stage of informational handling. The other three factors for measuring informational privacy concerns are context-aware processing, context-aware service delivery and context data storage. These latter factors could be identified and measured at the other stages of the informational handling procedure, that is, process, output and storage (Lee and Kwon 2010, p.5194).

In addition, the first factor, contextual data collection, consists of five concepts: concerns about the act of informational detection, diverse data collected, the level of

identifiable data, the various subjects that collect contextual data and collecting contextual data automatically without notice. The second factor, tracking and recording, is comprised of two concepts: concerns about tracking and recording technologies and about continuous tracking and the recording of events. The third factor relates to the sensors and infrastructure. It deals with two concepts: concerns for the possible embedding and disappearance of sensor devices and the sensing capabilities of sensors that could exceed human senses.

Furthermore, the fourth factor, context-aware processing, involves concerns about the prevalent risk of disembodiment of disassociation. This is because much more data is collected and autonomous decisions are made by the system on how and when to use or to pass on the information collected. The advances in artificial intelligence and data mining techniques heightened this concern. The fifth factor, the context-aware service delivery, comprises of concerns about a new context being automatically delivered by the system, being interrupted while processing and concerns for sensitive information. Finally, the sixth factor, the context data storage, deals with the concerns about the excessive storage of both sensor-based and high-level inferred context data.

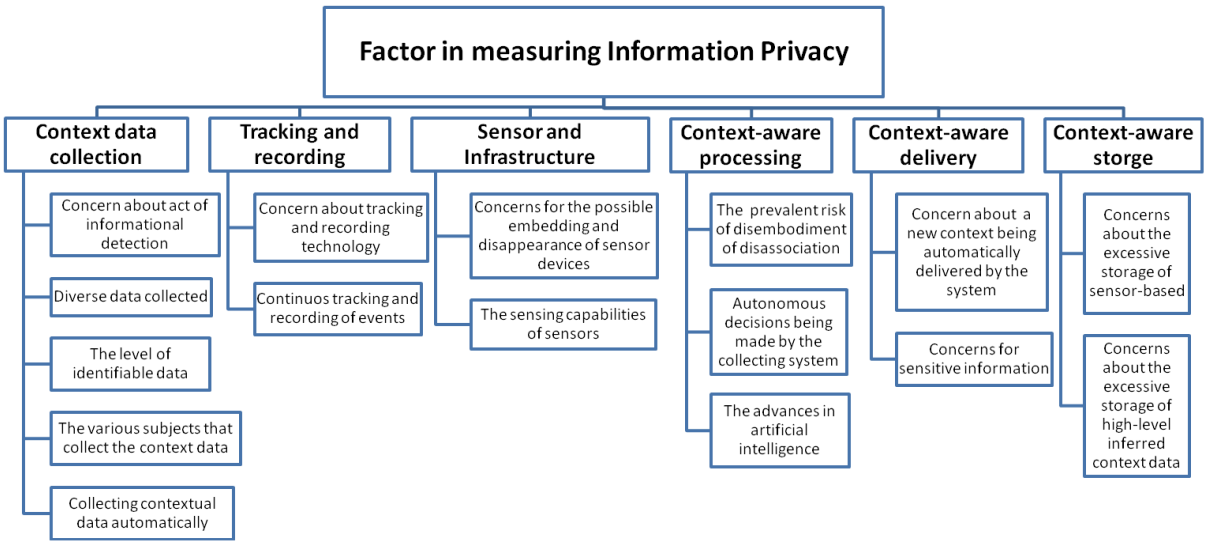


Figure 2-2: Factors on measuring informational privacy

2.2.3 PRIVACY AS A RIGHT AND VALUE

Rights entail two pairs of concepts. One pair is the claims and privileges, which represent a person's duties or absence of them. The other pair is the powers and immunities that characterize those who have and those who do not have power to alter others' claims and privileges (Volkman 2003, p.199). For example, with regard to privacy, if a person claims that no one, except his wife should know his income, then everyone has the duty not to try to learn how much he is paid, whereas his wife is the only person who has the privilege of knowing this information. This person has the power to either extend this privilege to include his friends, for instance, or to exclude his wife.

Values can be divided into three different types. The first, **instrumental values** are good because they lead to something else that is good. An example is the value of healthy diets, sports and friendship, which could lead to good health and happiness. The second type is **intrinsic values**, which are in themselves good, for example, health and

happiness themselves. The third type are **core values**, which are needed by all normal humans and cultures for survival and are considered common values for all human beings, such as, life, happiness and knowledge (Moor 2002, p.252). The author discusses three ways, summarised in the next three paragraphs, for justifying privacy using instrumental, intrinsic and core values.

Privacy might be considered an instrumental value if it leads to the good of protection from harm (Moor 2002, p.252). In other words, the practice of privacy would prevent unnecessary exposure of a person's sensitive information, for example, health information and thus prevent this person from being at risk of discrimination at work based on their health problems. Stahl (2008, p.53) adds that privacy is important because private space is essential to protect our social relationships and mental health.

However, according to Moor (2002 p.252) protection from harm is not a strong argument, as we can justify almost everything in our life as having this kind of instrumental value, even using toothpicks. Hence, Stahl (2008, p.52) argues that it might be more convincing if we considered privacy as an intrinsic value in which privacy would need no further justification. Moor (2002, pp.252-253) supports this idea by using the argument from Johnson (1998, p.89) who states that if we regard privacy as an essential aspect of autonomy, assuming that autonomy is itself an intrinsic value, we could argue, therefore, that privacy is an intrinsic positive value or at least the next best thing.

Stahl (2008, pp.52-53) adds that considering privacy as an intrinsic value would develop the secure and reliable identity of individuals and allow them to develop their autonomy. Moor (2002, p.257) continues the argument by presenting the example of situations where there is complete autonomy but no privacy, for example where someone looks at the history of the website addresses visited on his own PC, with no intention whatsoever of using, disclosing or even mentioning this very ordinary information to anyone. The argument, therefore, according to Moor (2002, pp.252-253) that privacy is considered an essential aspect of autonomy and that privacy should be considered as an intrinsic value is no longer very strong. Moor (2002, pp.252-254) then tries to use core values to justify privacy. He argues that as long as humans and their cultures need core values for survival, we could consider security as one such core value.

2.2.4 THEORIES OF PRIVACY

Westin's theory describes privacy as a dynamic process whereby people have the flexibility and freedom to regulate their own privacy when the need arises and a non-monotonic function, when, depending on their situation, people can choose how much or how little privacy they require (Margulis, 2011, pp.10-11). Margulis (2003, pp.243-261), however, argues that according to Westin's theory of privacy, privacy is not an end in itself but a resource for accomplishing a self-realization rather than a self-sufficient state.

In addition, Westin's theory of privacy consists of four concepts: freedom from others' surveillance (solitude), the ability to form a closed, relaxed, frank relationship group

(intimacy), the freedom from being identified in a public place and for public acts (anonymity) and the ability to limit disclosure to others (reserve) (Margulis 2003, pp.411-412 and 2011, pp.10-11). Marshal (1974) created a scale for measuring privacy known as The Privacy Preference Scale. It employed the four concepts of the Westin theory of privacy with two additional ones: the visual and auditory privacy of the home (seclusion) and not having anyone who would drop in without warning (not neighbouring) (Margulis 2003, p.413).

There are two further well-known theories of privacy: The Restricted Access Theory and The Control Theory of Privacy. These theories are described, critically evaluated and reviewed in a number of publications (Moor 2001, pp.89-91; Moor 2002, pp.249-262; Volkman 2003, pp.199-210; Elgesem 2004, pp.418-435; and Tavani and Moor 2004, pp.436-449).According to Moor (2001, pp.89-91), within the restricted access theory, privacy becomes a matter of limiting or restricting access to information about oneself in certain contexts, rather than keeping this information out of the minds of others. In the control theory, the unauthorized action of controlling others' information is not considered a privacy violation if the control of this information was not in one's mind. Elgesem (2004 pp.418-435), however, contends that inaccessibility within restricted access theory is not sufficient to maintain privacy, since it only limits the access of others to other individuals. There, therefore, could be restricted access but no privacy if somebody has the power to restrict people's informational and physical access to their own individual data but allow others to access to it. Elgesem supports his argument by giving an example of a prisoner, *an individual*, observed by guards, who, for their part, at the same time, restrict others from any informational or physical access

to this prisoner. Nevertheless, Elgesem acknowledges that restricted access theory would work if we view privacy as a relational concept in which relative privacy is applied with respect to specific individuals or circumstances, that is, guards or prisoners in his example.

Tavani and Moor (2004 pp.436-449) state that traditionally privacy of information is defined almost invariably in terms of control, for example, privacy is defined as the ability of the individual to control the circulation of information related to him/her. Alternatively privacy is the control we have over information about ourselves, rather that the complete absence of personal information. The authors argue that it is misleading to limit the definition of privacy to the action of control. They insist that there are many situations where others have access to information about us without violating our privacy, for example, our general practice doctor has access to our health history in order to provide us with a correct diagnosis. They claim that a good theory of privacy must account for the concept, justification and management of privacy.

2.3 PRIVACY, INFORMATION COMMUNICATION TECHNOLOGY AND CULTURES

A number of researchers have studied privacy concepts in different cultures, including Western (Volkman, 2003), Japanese (Nakada and Tamura, 2005 and Capurro, 2005), Chinese (Yao-Huai, 2005), Thai (Kitiyadisai, 2005) and Arabic culture, which falls within the Islamic perspective (Berween 2002, and Hayat, 2007). Other researchers have studied the organisational perspectives of privacy within the application and/or usages of CMC. Some of these researchers, for example, have investigated the organisational and individual perceptions of privacy within both public and private

organisations (Wilford, 2004). Other researchers have examined the role of IS/ICT staff toward both the formation and the application of a privacy laws, such as, the Privacy and Data Protection Act 1998 (Howley *et al.* 2004). Others have inspected the privacy policy of CMC applications, that is, within online activities (McRobb, 2006, Shallhoub, 2006a and Shallhoub, 2006b). Some researchers have made an empirical study of the relationship between privacy and control (Xu *et al.* 2008); between privacy and perceived vulnerability (Dinev and Hart, 2004); between privacy and perceived risk and of the informational privacy concerns model (Stewart and Segars, 2002, and Malhotra *et al.* 2004).

It is generally agreed that there is a common cultural understanding regarding privacy, particularly with respect to the opinion that privacy is a desirable and required right (Newell 1998, p.366). The effect, however, of cultural background on an individuals' perspectives towards privacy within ICT and CMC needs to be examined, particularly at the level of behaviour, as certain acts may be interpreted as a violation of privacy by some cultures but not by others.

Zakaria *et al.* (2003, p. 50) state that the design and use of ICT are directly affected by the cultural background of the nation(s) where they are designed and utilized. Hubona *et al.* (2006, p.200) argue that the use of ICT, particularly its adoption, is influenced by cultural factors, such as, social norms, beliefs and values. In addition, culture is considered to have an effect on the technology's outcomes, in other words, better beliefs about and attitudes towards technology lead to a better adaptation of the technology, in this case, the Internet, (Loch, *et al*, 2003, p.45) and its related issues, such as, privacy.

Yet, according to Ibrahim and Daing Ibrahim (2006, p.48), the frequency of internet usage among students from different ethnic groups, cultures and religions tends to show no significant variations. The relationship between ICT and cultural background is discussed in Section 3.1.

Newell (1998, p.366) has empirically demonstrated that although there are "hardly noticeable" cross-cultural differences in privacy definitions and functions, when other factors, such as, age, gender and sometimes income are taken into consideration, these differences do exist. Bellman *et al*, (2004 pp.313-324) found that differences in internet privacy concerns are due to differences in cultural values as well as the level of internet experience. Stahl (2008, pp.51-52) states that although there seems to be a consensus about the importance of privacy, its concepts and the reasons behind its importance are culturally varied. Similarly, Collste (2008 p.76) argues that privacy has various concepts, not just between Western and Eastern views, but also within Western perspectives themselves.

2.3.1 PRIVACY AND ICT

The relationship between privacy and technology could be studied from two perspectives. As it has been mentioned in (section 1.2), one perspective concerns the role of technology (specifically ICT) when considering the concept of privacy. For example, Internet users face exposure to a wide range of information gathering techniques while they search the internet (Clarke 1999 p.60; Kelly and Rowland 2000, p.4). A different perspective addresses the role of technology, that is, in terms of privacy-enhancing tools (PETs) (Tavani and Moor 2004, pp.436-449) and privacy seals

(Moores, 2005, pp.86-91) in obtaining the desired level of privacy within ICT applications.

In terms of the role of technology in raising concerns regarding privacy, it has been argued that ICT has this impact on privacy for two reasons: one is a function of the way it speeds up the already extant actions of collecting, processing and exchanging personal data. The other reason is its capacity to put information together in a way that could negatively affect people, that is, cause them physical, emotional, financial or legal harm (Stahl 2004, pp.5-6).

Clarke (1999, p.60) outlined a number of real-time information gathering techniques that invade the private space of cyberspace users. Among these techniques are spam, cookies, click-stream and biometric identification techniques. Kelly and Rowland (2000, p.4) outline a number of examples of information gathering technologies that are used by webmasters to collect information about web visitors. Within these techniques, a range of personal and technical information about web visitors and their personal computers are collected. For example, by browsing a website, information about the type of browser, operating system and internet protocol used by the web visitor would be recognized by the webmaster even for anonymous users. Nevertheless, those web visitors, particularly electronic commerce (e-commerce) customers, are often required to provide personal information including their name, address, age, income and gender if they want to gain access to some websites or to gain entitlement to promotional offers (Kelly and Rowland 2000, p.4).

In terms of the role of technology in obtaining the desired level of privacy within ICT applications, PETs are considered a technological way of getting nearer to the desired level of privacy within ICT applications. Tavani and Moor (2004, pp.436-449) maintain that PETs serve as an alternative solution for two extreme claims proposed by internet users and the e-commerce sector. On the one hand, internet users demand strong privacy legislation to protect their interests and right to privacy online whereas on the other hand the e-commerce sector calls for self-regulation to protect privacy (Tavani and Moor, 2004, pp.436-449). Authors describe PETs as two embedded concepts: technical, that is, online tools and organizational, that is, industry-standard guidelines for the protection of personal identity and, therefore, the protection of privacy.

In addition, Senicar *et al.* (2003, pp.151-155) outlined a number of the PET technologies that included encryption, e-profiling, embedded software, trust centre, identity protector, cookie management and an anonymizer. Tavani and Moor (2004, pp.436-449), however, argue that PETs are not always sufficient to provide adequate privacy protection. This is because the anonymizing tools provided by PETs do not always have total anonymity, especially in the websites that provide these tools.

Privacy seals programmes, such as; TRUSTe and CPA WebTrust are considered an organisational way to obtain the desired level of privacy on the Internet. These programmes are developed by the e-commerce industry to build trust between the e-commerce sector and its customers (Moores, 2005 pp.86-91). Within these programmes, applicants for privacy seals for such websites have to go through a number of processes that include writing a privacy policy and completing a self-assessed questionnaire on

their business practices. Each application is reviewed and approved by the trust organization, that is, the programme provider. In addition, the applicant website must agree to abide by the principles of the relevant privacy seal programme and display the agreed privacy policy on their website, including details on the use and sharing of the users' data (Moores, 2005 pp.86-91).

Finally, these websites must provide adequate security measures to protect the user's information (Moores 2005, p.88). Moores (2005, p.89) argues that the privacy seal programmes are limited because they lack real power on the part of the trust's organization to deal with abuse. For example, they are unable to curtail situations of abuse, such as, selling customer databases as part of the trade of the website owner, which could be legally covered by including the relevant conditions on the privacy statement of some websites.

There is a relationship between privacy concerns among Internet users and their familiarity with practical ways of controlling their privacy online. The familiarity increases with an increase in the level of Internet usage (Bellman *et al.* 2004, p.316). In addition, there is a relationship between Internet literacy and concerns about privacy. Internet literacy is defined as, "The ability to use an Internet-connected computer and Internet applications to accomplish practical tasks." (Dinev and Hart, 2006, p.9), in conclusion, these researchers argue that greater Internet literacy will make users more competent in protecting their computers as well as their personal information and, therefore, make them more concerned about their privacy.

2.3.2 ICT AND CULTURES

Culture might be defined as "*the heritage of learned symbolic behaviour that makes humans human*" ((Keesing, 1974, p. 73), however, this definition includes too much that would be difficult to interpret and analyse, and therefore it is very useful to narrow down the meaning of culture (Keesing, 1974, p. 73). Moreover the challenge in studying culture isknowing how to narrow its concept in a way that includes less and reveals more. A culture cannot be defined only by the behaviours that are learned across generations and shared by people in a particular society which make them human; rather it could be defined as an adaptive or as an ideational system (Keesing, 1974, p. 73). In terms of looking at culture as an adaptive system, culture according to an adaptation point of view is considered a system, and its change is measured as a process of adaptation, in which technology and economy are the most adaptively central area of this culture, whereas the ideational view of culture considers culture as a cognitive, structural or symbolic system. For example culture should consist of one's belief that one needs to operate in an acceptable manner among peers. Such knowledge will help the members of the culture decide what the action is, and how they feel about it. (Keesing, 1974, Schwartz, 2006 and Smith et al, 2011)

Hofstede (1984, p.18 from Zakaria *et al.* 2003, p.52) describes cultural value as "A broad tendency to prefer certain states of affairs over others." Schwartz, 2006, on the other hand, defined culture as "a rich complex of meaning, belief, practices, symbols, norms and values prevalent among people in a society" (Schwartz, 2006, p.p 138-139). The cultural value is the most central feature of a culture and it shares the meaning of

what is good and culturally ideal. Moreover it has been claimed that there is a link between value and behaviour (Smith et al, 2011)

Culture could include facts, symbols, norms and values in a particular society, and guidance within a culture could come from the individual's own expertise, social sources such as superiors, relatives and friends, rules and law, and the individual's beliefs based on the religion or ideology of the culture (Smith et al, 2003, p.191), therefore it can be described as, *"The quintessence of the physical resources and perceptions of the physical and mental techniques, which allow a society to persist."* (Stahl and Elbeltagi 2004, p.48).

In addition, Bellman *et al.* (2004, p.315) describe cultural values as a set of beliefs that influence behaviours. The authors emphasise that these values should remain unchanged within a particular culture regardless of any economic, political and technological changes within it. Zakaria *et al.* (2003, pp.52-53) add that the values of members of a particular cultural group tend to influence indirectly their behaviour via their attitudes and goals, such as what they view as the good life (for people in highly individualistic cultures) or helping others and producing a better society (for highly collectivist people). Consequently, these values influence the level and manner of adoption of advanced technologies such as ICT applications.

Ajzen (1991, in Baker *et al.* 2007, pp.359-362) argued in The Theory of Planned Behaviour (TPB) that the intention to use technology and consequently the level of usage of it within a particular cultural group, depends on three factors. The first one is

the attitude of these cultural group members towards such behaviour (i.e. using new technology). The second one is their subjective norms (which is the expected social pressure from one's peers or superiors to accept this new technology). The third one is their perceived behavioural control (i.e. the availability and importance of sufficient skills, resources and opportunities to use this technology). Baker *et al.* (2007, p.360) add that gender, age and level of education might influence the above-mentioned factors.

A number of researchers have identified the relationship between cultural background and patterns of Internet activities, for example, online purchasing trends of consumers (Chan *et al.* 2002, p.139). In addition, it is argued that the way information technology is used to transmit information is affected by human relationships (Zakaria *et al.* 2003, p.57).

A study of students from Malaysia, China and India by Ibrahim and Daing Ibrahim (2006, pp.40- 49), showed that although ethnic origin has no appreciable influence on the level of Internet usage among students of diverse cultural and religious backgrounds, there were differences between students from these ethnic groups at the level of e-mail usage. Interestingly and with respect to Arabic culture, Hill *et al.* (1998, cited in Baker 2007, p.358) found that new technologies tend to be introduced to Arabic organizations by young Arabs who have used these technologies in a developed country.

The relationship between ICT and culture has been studied from the managerial perspective by a number of theories such as The Theory of Planned Behaviour (TPB), Technology Acceptance Model (TAM), and Diffusion of Innovations (Lee et al, 2003 and Greenhalgh et al, 2004). The following is a brief description of these IS theories.

The theory of planned behaviour, TPB, which was originally, developed from the theory of reasoned action TAR study, mainly the individual's intention towards such behaviour (Ajzen, 1991, pp. 179-211 and Conner and Sparks, 2005, 170-222). TPB claims that behavioural achievement depends on the personal motivation, such as the individual ability and subjective norm, which could be measured as factors for behaviour (Ajzen, 1991, pp. 179-211).

Regarding the TAM, which was also developed from TRA (Ajzen and Fishbein, 1980 and Davis *et al*, 1989, p.985), it studies the individual's acceptance of information systems. Moreover TAM principles are driven from the assumption that the individual's information systems acceptance could be measured by two main factors, which are the perceived usefulness and perceived ease of use, and a number of additional factors such as voluntariness, complexity, accessibility, and computer anxiety, as well as demographic factors such as gender (Lee *et al*, 2003). In addition privacy concerns have been studied in some IS research using TAM. For example, studying Trust and TAM in Online Shopping (Gefen *et al*, 2003), Adoption of Biometric Technology (Elgarah and Falaleeva, 2005), and An Examination of Individual's Perceived Security and Privacy of the Internet in Malaysia (Lallmahamood, 2007).

Regarding the diffusion of innovations theory, it could be defined as the study of the acceptance, revision, and use of technology. It is mainly used to study the barriers to the diffusion of such technology. Moreover the diffusion of innovations theory intends to study the differences in understanding such technology between the agency that introduces it and the intended users. It also studies the relationship between the interaction of the innovation and its potential context in such an environment, which is called "innovation-system fit" (Greenhalgh et al, 2004, pp. 581-629).

Given that this research is not management based research and is not about accepting technology, these theories do not fit with the research aim (section 1.3) or questions (section 1.4) .

2.3.3 PRIVACY AND CULTURES

The distance between public and private affairs was entrenched in the culture of ancient Greece by Socrates, Plato and Aristotle (470-322 BC) and in Ancient China by the Warring States (403-221 BC) (Kemp and Moore 2007, pp.59-60).

As mentioned before, the perception of privacy within Western culture can be described, according to Judge Cooley, as the right to be let alone and extended to ICT and CMC, the right to informational self-determination (Stahl 2004, p.63). Privacy, however, as a concept is arguably still not clearly understood (Fairweather, 2001).

The concept of privacy as it might be found in Western culture, does not exist in Far Asian cultures, that is, Chinese, Japanese and Thai cultures (Brey 2007, p.15). The

author argues that these cultures are collectivist rather than individualistic. They tend to be interested in collective values more than the individualistic ones, which would conflict with the privacy concept as an individual right (Brey 2007, p.15). Within modern China, however, there has been a gradual increase in the individual's expectation of the right to privacy for him/herself as well as for others. The meaning of privacy has been extended to include all personal information rather than just the shamefully secret, which is the traditional and narrow meaning of privacy (Yao-Huai 2005, p.8). These new notions of privacy have influenced the regulation of the right to privacy in the Chinese legal system, for example, Article 40 of the Chinese Constitution protects its citizens' rights to freedom and privacy in communications, however, there is no national data protection law in the Chinese legal system (Yao-Huai 2005, pp.9-10).

Japanese culture attaches less importance to the right to privacy than the West due to cultural and linguistic differences. For example, the Japanese equivalent of the private versus public dichotomy in Western culture is the dichotomy of the partial, secret and selfish versus the public (Brey 2007, p.15). Concern about the violation of privacy has emerged in recent times (Orito *et al.*, 2008).

Cultural backgrounds could affect online trust and privacy. Some researchers suggest that embedded cultural value tends to affect the level of trust, while others claim that an individual's beliefs and, therefore, their decision to use the Internet for online shopping is affected by sharing a common value with other individuals via what is called an in-group trust culture (Siala *et al.* 2004, p.7).

Cultural value could be described as one of the reasons behind the differences in the level of concern about Internet privacy (Ballman *et al.* 2004, p.313). There is also a relationship between the level of trust in society and the level of reliance on families as a source of the trust (Dinev *et al.* 2005, p.2). In addition, privacy perceptions are connected to aspects of an individual's social group. Xu *et al.*, (2008, p.7) demonstrate that the social norms of Internet users could be used to predict the nature of their privacy values.

With regard to Islamic culture, the concept of privacy has been recognised by Islam in a number of verses of the Islamic holy book, the Qu'ran. For example, in the verse that insists that people do not enter the houses of others without gaining permission from the owner.

In Arab culture, religion tends to play an essential role and affects most people's life and business decisions (Zakaria *et al.* 2003, p.57). Trust in religious groups is usually engendered through cultural values, that is, the teachings of parents, older generations and ministers or clerics of the religion (Siala *et al.* 2004, p.10). These researchers add that within the Muslim religion, in-group trust effects can transfer to online attitudes.

Islamic countries observe ethical issues relating to technology from the perspective of Islam, for example, the Islamic Body on the Ethics of Science and Technology, which was created by the Ministries of Higher Education and Scientific Research of Islamic Countries, directs Muslim public opinion on the important ethical issues in computing, including online privacy, from the perspective of Islam. In addition, Muslims appears to

adhere more to computer codes of conduct that come from Islamic teaching compared to those that emanate from other sources (Al-A'ali 2008, p.29).

It appears that there is an association between the level of government involvement with regard to information privacy regulations in a country and the level of concern about privacy among Internet users in that country (Bellman *et al.* 2004, p.315). Furthermore, a positive relationship between government and corporation involvement in privacy regulation and privacy concerns has been identified, for example, online corporate policies provided by companies with the support of a legislative framework through government regulation tend to reduce an individual's online privacy concerns (Milberg *et al.* 2000, and Wirtz *et al.* 2006, pp.340-341). However, private governance of the privacy regulation by corporation affect the realism and fairness of these regulations, and therefore affect the privacy concerns (Peek, 2007, pp. 165-166). The effect of the power of both the state and the corporation on the privacy concern is covered in the following section (section 2.3.4).

2.3.4 PRIVACY AND POWER OF THE STATE

Milberg *et al.* (2000), and Wirtz *et al.* (2006, pp.340-341) argue that a relationship exists between the online users' privacy concerns and the regulations proposed and imposed by governments and corporations. Such regulations could be explained as the coming from power of state (Peek, 2007, p. 136) and corporation (Peek, 2007, p. 139 and pp. 165-166). In this section, the state and corporation as well as their power on the society will be defined and the relationship of both; the state and corporate powers, with the online privacy, will be briefly explained.

A state has been defined as a political body that consists of people, region, government, economy, military and rule (Kuthy, 2011, pp.17-18). This body is authorized, by God, the People, or The Monarch, to propose and implement rules and regulations for the overall benefit and well being of all of its constituents and the power to enforce such rules and regulations. The legitimacy of using power within such a state is controlled by the political body (Kuthy, 2011, pp.17-18). A corporation has been defined as an exclusive business body that aims to maximize its owner's or investor's profits, in a way that could conflict with many values of its community such as employee income, and costumer privacy (Peek, 2007, pp. 137-138).

The power of state could be defined as a despotic or infrastructural power. The despotic power of the state includes the actions to gain the authorisation to facilitate and control the cooperation within the society's groups, whereas the infrastructural power is the ability of the state to implement democratically political decisions thorough the society (Mann, 1984, pp. 126-128, Kuthy, 2011, p.21). The corporate power, on the other hand, could be defined as a type of power to domestically and/or globally control governments and/or legislation. The corporate power has a number of forms, for example, it could be a direct violation of a law due to the weak governmental reaction to such violation, or it could be a misinterpretation of the government legislations. Corporations take advantage of the inability of these weak governments and their silence and inaction to such behavior to serve the primary interests of its investors or to primarily satisfy its own interests (Peek, 2007, p. 143). The corporate power can also be the ability to directly cause changes to the law in its own interests. For example the

International Olympic Committee forces host nations to accept law changes to protecct the interests of advertisers in exchange for being allowed to host the Olympics. Business interests - notably the Disney Corporation - in the US forced a change to copyright law[2].

With respect to the online privacy, the individual perspective and concerns regarding information privacy are affected by the regulation proposed and implemented by both state and corporations. Peek (2007) claims that information privacy is controlled by the regulation of both the governmental law and corporate governance.

Regarding the online privacy concerns caused by the power of state, the problem of the power of state could be in the developed regulation and law, for example the American privacy law cause concerns on the middle-class. Although, the American privacy law has been established to prevent the misuse of the collected personal information, the law causes concerns for those with low-income during the ongoing interpersonal data collection in exchange for the government welfare program. (Gilman, 2008, p. 27 and Gilman, 2012, pp. 1392-1394).

Another online privacy concern caused by the power of corporations is the personal data collection. The problem occurs due to the nature of the modern internet practices, in which the personal data serves as a price for online services and becomes a profit

[2] http://en.wikipedia.org/wiki/Mickey_Mouse_Protection_Act

element to the data collectors (Mitchell, 2012, p.10, and Solove, 2013, p.11) This problem is compounded (exasperated) by the inability of the law to cope with the development of internet technology (Mitchell, 2012, p.2). Consequently, internet users hold a minimal negotiating power with regards to giving up their personal data and face coercion to exchange their data for the online service with either take it or leave it and in many cases the leave it option is not possible (Mitchell, 2012, p.10 and Solove, 2013, pp.11-13).

Although the main corporate power comes from the government support and collaboration, corporations gain power also, with the aid of certain corporate actors who propose and design the legal systems. This would be done by the control of an interlocking web of actors, from both the governments and corporations, but not from the other members of the society, such as its citizens. In addition corporations gain power by dominating the interpretations of reactions to the privacy regulation (Peek, 2007, pp. 126-169).

With regards to the developing countries, Lamer (2012) argues that the state have the power over ICT and media, which used mainly in despotic governments, for example by blocking search engine or taking action against enabling the encryption technology in Blackberry services (Bremmer, 2010, p.4).

In conclusion the state and corporate power holds dominion over the individual and exerts enormous power both domestically and globally. Moreover, the role of the privacy laws is to legitimize the existing privacy practises proposed and designed by the

corporations. This is not surprising as in E-commerce; the individual's personal information is essential material for the development and therefore the success of such business (Peek, 2007, pp. 126-169).

In this research, internet regulation is considered as the regulation that is directed by both government and corporations (Ehereneich, 2001).

2.4 ONLINE PRIVACY PERSPECTIVE

As referred to in section (2.2.5), the spread of Internet usage and online communication has changed the vision of privacy. In particular the possibility of having private communication online compared to offline. This is due to the mechanical nature of the Internet, which is able to retain and reveal private online conversations. The study of privacy online, therefore, becomes imperative (Walther 2011, p.3).

The interest in privacy online extends to the nature of the information that is disseminated i.e. personal information, information about the provider (their age, gender, level of study and ethics) and the information collector (e-commerce, e-government and social networks) (Smith *et al.*, 1996, p.189). In this section, the role of the nature of the information, the provider and the collector are described.

2.4.1 ONLINE PERSONAL INFORMATION

Online data could be categorized into four types (see figure 2.3): personal data, such as, name, address, telephone number and e-mail address; sensitive data, such as, religion, nationality and political opinion; identification data, such as, identification card number and DNA and anonymous data, such as, gender and age (Guarda and Zannone, 2008,

p.7 and Ghani and Sidek, 2009, p.411). As mentioned earlier, the type of information provided affects the level of privacy concerns (Smith *et al.*, 1996, p.189) and it has been claimed that Internet activities could be decreased because of the nature of the personal information required to be submitted in order to complete these activities (Dinev and Hart, 2003, p.6). Personal information in terms of the online context is defined as the information essential for completing an online task or transaction (Dinev and Hart, 2006, p.31). Personal information includes information, such as, name, address and credit card number.

In addition Ganow and Han (2010, p. 305) propose three categories of personal information; high-risk, mid-risk and low-risk data. The high-risk data includes any data that can be used, alone, to identify and therefore cause harm to a particular individual, whereas the mid-risk data are the combination of data that can be used together to identify and cause harm to an individual, and the low-risk data cannot identify an individual without the presence of high-risk or mid-risk data. Ganow and Han (2010, p. 305) argue that this classification provides an operational process that allows cooperation to ensure privacy protection.

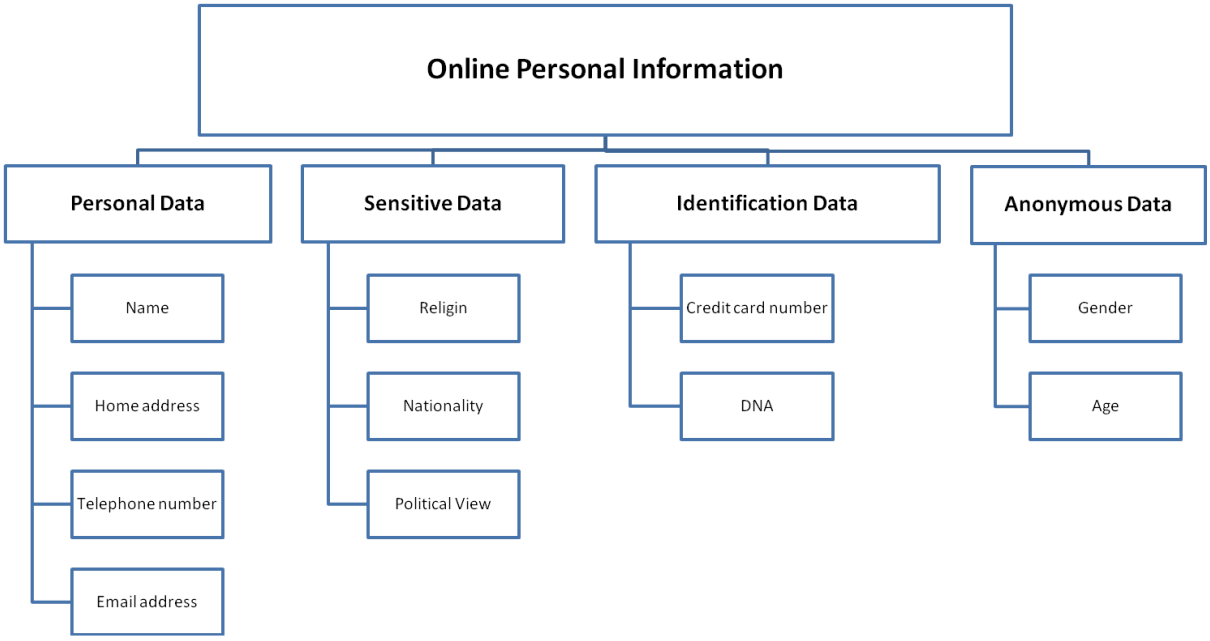


Figure 2-3: Online Personal Information

Furthermore, it is argued that the level of privacy concerns is related to the type and amount of personal information that is required to be submitted in order to complete online tasks or transactions. Furthermore, the type and amount of personal information required could be used to divide online tasks or transactions into six levels of Internet activities: surfing, communicating, registering, shopping, banking and seeking answers (Dinev and Hart, 2006, p.32).

2.4.2 ONLINE PERSONAL INFORMATION PROVIDER

Various studies have examined the relationship between gender and Internet privacy concerns. Some researchers suggest that females anticipate a possible negative outcome as a result of providing their personal information via the Internet (Slovic *et al.*, 1997 from Garbarino and Strabilevitz, 2004, p.770).

Furthermore, females are more concerned than males about the loss of their privacy while they are online (Bartel-Sheehan, 1999; Kehoe *et al.*, 1997 from Garbarino and Strabilevitz, 2004, p.770). Other researchers (Liebermann and Stashevsky, 2002, p.297) claim that females perceive higher risks than males when they submit personal information such as credit card details to a website.

In addition, Garbarino and Strabilevitz, (2004, p.771) state that statistically females take their online privacy more seriously than males, however, the authors suggest that the gender difference in online privacy concerns relates to the consequences of losing privacy rather than the likelihood of such privacy being lost. It is argued that the study of the gender factor should not focus exclusively on the differences between men and women, rather it should be focused on how such differences would lead to the unequal distribution of power (Gillard *et al*, 2008, p. 265). Moreover, although it is agreed that the distinction between male and female (or men and women), which returns to the biological differences, serves as a basic classification and stereotype in some cultures, and therefore might produce an inequality among them (Bem, 1981, p. 354, and Gillard *et al*, 2008, p. 264), there are other cultural factors that could increase the inequality between men and women. These factors could be illiteracy, overwork and sexual violence that women suffer in some societies (Gillard *et al*, 2008, p. 265).

In addition, a number of researchers argue that most of the gender studies confirm rather than challenge gender inequality (Howcroft and Trauth, 2008, p.187) and therefore they propose the use of Feminist research approach. Feminist research is considered critical research in which they provide a critical perspective of such a phenomena with the

intention of providing a social change element (Howcroft and Trauth, 2008, p.186), however social change is not one of the objectives of this research and therefore, feminist research is not applied in this research.

With regard to the effects of age and educational level, Liebermann and Stashevsky (2002, pp.297-298) claim that older people as well as those with a lower level of education perceive higher risks from submitting their personal information.

2.4.3 ONLINE PERSONAL INFORMATION COLLECTOR

One of the factors that affect the level of privacy concerns is the personal information collector or keeper, that is, the organisation requesting the information and their websites (Smith *et al.*, 1996, p.189). The ability of websites to collect information about a visitor without this being noticeable to the visitor has increased concerns surrounding online information privacy among Internet users (Bellman *et al.*, 2004, p.314). Internet activities, therefore, could be reduced as a result (Dinev and Hart, 2002, p.6).

The Internet trust issue is relevant when there is a possibility of risk or if there is an element of uncertainty in the relationship between Internet users and the websites they are using. It has been proposed that willingness to conduct online activities is affected by the level of trust (Siala *et al.*, 2004, pp.8-9). Trust in how websites handle and protect personal information was found in general to be very low, for example, only 6% of US consumers trusted websites to handle their personal information correctly (Dinev and Hart, 2006, p.9).

Online trust is the level of confidence among Internet users with regard to how their personal information will be used. Online trust can be affected by the belief that the user's personal information will be kept safe (Dinev and Hart, 2006, p.66).

2.5 THE STUDY CONTEXT

As it has been mentioned in the introduction chapter, (1.2 Online Privacy and 1.5 The Significance of the Research) there is a lack of studies into the affect of religion belief, and social norms on the online privacy perspective of Internet users in Islamic countries and therefore this research is a step forward to study the cultural effects on the perspectives of individuals with regard to the relationship between privacy and Internet usages, in Islamic countries. In order to conduct this study, populations with specific characteristics are targeted. These characteristics include being a Muslim, with a minimum education level and represent either Arabic or Eastern cultures.

In addition the selection of Muslim as a target participant is important to have the religion as a constant and therefore eliminate the variation that could come from the differences between the religions and concentrate on the identifying of these differences that come from the cultural perspective of the affect of the religion believe on the online privacy perspective. With regards to the education level, the minimum set to be the undergraduate level, which aims to reduce the affect of illiterate on the online privacy perspectives within the participants and concentrate on those differences that come from age and gender rather than variation in education levels. Finally, the research has been designed to target two different cultures within the Islamic world, which are the Arabic and Eastern cultures. Such design would provide an opportunity to examine the effect of cultural background, i.e. Nationality on the online privacy perspective, and to compare

the effects of social norms, religion believes, Internet regulation and IT skills on the online privacy attitudes between the two cultures, Arabic and Eastern cultures.

Thus the target participants are Muslim students and members of staff at higher education establishments from the two Islamic countries, Saudi Arabia as an Arabic country and Malaysia as an Eastern country.

The aim of this part the chapter is to provide a background review of the countries from which the target participants were drawn i.e. Saudi Arabia and Malaysia. The review begins with general information about each country, including their location, population and political system. The Internet services, infrastructures and the privacy regulations of each country are then discussed in order to provide background information about the research area and the privacy perspective of Internet users. Finally, a description of the higher education system in each country is given to provide information about the nature of the sample population for this research.

2.5.1 SAUDI ARABIA

King Abdul-Aziz Al-Saud founded the Kingdom of Saudi Arabia on September 1932. The country is located in the southwest corner of Asia and it spread over 2,150,000 square kilometres (830,000 square miles). As the largest country in the Middle East, it occupies four-fifths of the Arabian Peninsula. On September 2004, its population of Saudis reached 22.7 million (Ministry of Foreign Affairs, Alexander, 2011, p.199).

Saudi Arabia is a monarchy, headed by the Al Saud royal family, with a council of ministers. The political system in the Saudi Arabia is based on Islamic and Arabic laws

and the source of its legislature are the religious and tribal histories. Saudi Arabia is considered the keeper of the Islamic religion with responsibility for preserving it. For this reason, Saudi Arabia uses the Qur'an and the Prophet's Hadith (written record of Prophet Muhammad's practices and made of life) as the basic law of the government (Ministry of Higher Education Portal and Baki, 2004, pp.2-3, and Al Lily, 2011, pp.119-127). In other words the legal system in Saudi Arabia is based on the Holy Qur'an and the Hadith (Ministry of Higher Education Portal).

Until the discovery of oil in the 1970s, Saudi Arabia was economically, politically and militarily weak; however, since then it has become a strong country and has enjoyed a major economic boom. Nowadays, Saudi Arabia is one of the richest countries in the world, playing major economic and international roles.

2.5.1.1 Internet in Saudi Arabia

Although Internet was introduced in Saudi Arabia, initially, in 1994, its use was limited to academic and medical researchers. Public access to the Internet was delayed until 1999 when local Internet service providers established a filtering system for any inappropriate and unwanted content. Since then, Internet services have become available to the general citizenry. Recently the Internet seems to have played a great role in bridging the public-private division of Saudi society and encouraging, particularly the Saudi women, to communicate with members of the opposite gender (Petrson and Ulferts, 2011, p.19, and Al Lily, 2011, pp.119-127).

2.5.1.2 Higher Education in Saudi Arabia

The development of universities began in Saudi Arabia began in the 1950s under the management of the Ministry of Education. Women, however, did not gain access to formal higher education until the 1970s. Since then, they have studied at separate campuses, taught face-to-face only by women. They are allowed to be taught by male academics via closed-circuit television (CCTV) (Al Lily, 2011, pp.119-127).

In 1975, universities became separate education entities under the Ministry of Higher Education and by the late 1990s; Saudi Arabia had seven public universities with 68 colleges for men and 61 for women. Nowadays, there are 21 public universities (Kahlid and Mohamood, 1997, p.156, Alexander, 2011, p.199, and Ministry of Higher Education Portal). In 1999, the number of graduates from Saudi universities was 42,950 with 58% being female compared to only 808 in 1970 with as little as a 1.6% share in female students (Baki, 2004, p.4-6).

2.5.2 MALAYSIA

Malaysia occupies an area of land originally known as the Malaysian Kingdoms of the 18th century. It eventually became a British colony. Malaysia gained independence from Britain in 1957. It started as the Federation of Malaya and in 1963, it formed a new union with Sabah, Sarawak and Singapore but in 1965, Singapore left the union and become an independent country. Malaysia is now a federal constitutional monarchy and is part of one of the most active economical regions in the world i.e. Asia. Malaysia is located on the south-east coast of Asia and covers 329,847 square kilometres (127,350 sq mi). It has a population of over 26 million people of various ethnicities and religions. The Malaysian nation comprises of a multi-ethnic and multi-religious people

where the major ethnic group are Malays (50.3%), Chinese (23.8%), non-Malaysian original people (11.0%) and Indians (7.1%) (Lim and Har.,2008, p.29, Zaaba *et al.*, 2010, p.189, Ibrahim *et al.,* 2011, p.1004, Kasim *et al.,* 2011, and Wikipedia**).**

2.5.2.1 Internet in Malaysia

Initially, the Internet was introduced in Malaysia in 1990. It then gradually spread over the next six years until in 1996. Then the speed of the Internet spread accelerated because of the government's engagement in ICT development. Consequently, the annual average increase in Internet users reached 134.9% in 2000-2004, with 8.7 million users. By 2007, the Malaysia Department of Statistics recorded that 23.4% of the whole population had become Internet subscribers (Xue, 2005, p.243, Ooi *et al.*, 2011, p.2, and Jehangir *et al.,* 2011, pp.171-172).

2.5.2.2 Online Privacy in Malaysia and Privacy Regulation in Malaysia

Malaysia has enacted six cyber laws: Digital Signature Act 1997, Computer Crime Act 1997, Telemedicine Act 1997, Communication and Multimedia Act 1998, Communication and Multimedia Commission Act 1998, The Copyright Act 1997 and Electronic Commerce Act 1997 (Jehangir *et al.,* 2011, pp.171-172) to increase privacy and security. In spite of these Malaysia tends to have insufficient privacy protection, due to the absence of the right to privacy in the constitution and cyber laws themselves (Ho *et al.,* 2010, p.3).

The development of data protection law in Malaysia started with a first draft in 2000, then a second draft in 2007, followed by a first reading in 2009 and then a second and

third reading in early 2010, with a final reading in June 2010. This law is designed to protect personal data, which is collected by commercial transactions but not by federal and state government and data processed outside Malaysia, from being misuse (Hasbullah *et al.*, 2011, pp.311-313 and Roni *et al.*, 2011, p.314).

2.5.2.3 Higher Education in Malaysia

Until late the 1990s, there were only seven public universities in Malaysia, the University of Malaysia, University Sains Malaysia, University Kebangsaan Malaysia, University Pertanian Malaysia, University Teknoloji Malaysia, University Utara Malaysia and the International Islamic University (Kahlid and Mohamood, 1997), however, currently the number of public universities has risen to 20 (http://www.etawau.com/edu/IndexUniversityGovernment.htm). Ooi *et al.*, 2011, p.2 argue that the private higher education sector in Malaysia has the same government support.

After independence Malaysia continued to use English as its official language for ten years, alongside the Malaysian language, however, since 1970, English has been the second language. The English language is widely used in the business and higher education sectors, for example, the University of Malaya (UM), which is oldest university, established during British colonial rule, still continues to teach technology and some of its science courses in English (Zaaba *et al.*, 2010, p.189).

2.6 CONCLUSION

The aims of this chapter were to provide a literature review on online privacy as the area of investigation of this research as well as country context reviews of the target population of this research.

In the online privacy literature review, the concept of the privacy was discussed in detail, including a definition of privacy, informational privacy and online privacy, as well as the factors for measuring informational privacy and privacy theories. In addition, the relationships between privacy, ICT and culture were evaluated and then the online privacy perspectives including the role of the nature of online personal information, the online information-provider and information-collector were reviewed.

Although the study of the privacy concerns and Internet trust as calculus of the online privacy perspective (Dinev *et al.* 2005, p.2) and affect of age, and gender (Guarda and Zannone, 2008, p.7 and Ghani and Sidek, 2009, p.411) on the online privacy perspective have been cover in the literature review, it appears that there is paucity on the studies of the affect of the cultural background on the forming of the online privacy perspective. The lack on the literature about the online privacy perspective includes studies that cover the Arabic culture and Islamic world. Therefore a study of the cultural affects on the online privacy perspective within different cultural backgrounds needed. This research, hence, investigates the cultural affects on the online privacy perspective of the Saudi and Malaysia Muslim.

The country context reviews of Saudi Arabia and Malaysia, the countries from which the target participants were drawn, was brief. It summarized each country's location, population, political system, their Internet services, privacy regulations and higher education systems. In order to conduct this research and study the cultural affects on the online privacy perspective of the Saudi and Malaysia Muslim, an appropriate research methodology need to be applied. The following chapter reviews the research methodology for IS and social research. This would include the description of the ontological and epistemological considerations the philosophical paradigms, the quantitative and qualitative research strategies, and research methods and data collection techniques.

3 CHAPTER 3: RESEARCH METHODOLOGY

3.1 INTRODUCTION

In the preceding chapters, the motivation, aims and background to the area under investigation were discussed. As previously mentioned the aim of this research is to explore the relationship between online privacy perspectives and Internet users' cultural background, which includes the Internet users' social norms, religious beliefs, the Internet regulations in their country, their IT skills, nationality and gender (see 1.2 Online Privacy) and how it is affected by the cultural backgrounds of individuals in Islamic cultures.

In order to accomplish the aim of this research and explore the relationship between online privacy perspectives and Internet users' cultural backgrounds these areas of study, a number of research questions have been formed. The first and second research questions aim to determine whether there is a relationship between the level of an individual's concern and trust over Internet privacy and the effects of their religious beliefs, IT skills, social norms and local Internet regulation. The third question endeavours to understand how individual religious beliefs, IT skills, social norms and local Internet regulation affect Internet privacy concerns and Internet trust. The fourth question aims to highlight the similarities and differences that exist between Muslims from different cultural backgrounds using Saudi Arabia and Malaysia as exemplars with regard to the effects of their religious beliefs, IT skills, social norms and local Internet regulation.

Answering the above-mentioned questions in academic terms required using a research methodology that is appropriate for research into information systems and the social sciences. This chapter, therefore, provides a literature review on research methodology for IS and social research. It is arguable that there is no single correct way to produce a good piece of social research writing but it is rather a combination of strategies and methods. There are a number of key decisions to be considered when undertaking such research. A crucial key decision is whether the research itself is relevant to the current social issues of interest as well as the question of whether the expected information gained would build on existing knowledge. In addition, researchers are required to be able to answer other questions with regard to their expected findings. For instance, regarding accuracy, objectivity and ethical issues, researchers should ensure that their studies have produced honest, fair and balanced findings that do not affect the rights of the participants (Denscombe, 2010, pp.3-5).

This research can be classified as social research. It could be further classified as academic and applied research, as a piece of academic research; its motivation is to develop a theoretical explanation for social phenomena. As applied research, its purpose is to find a solution to social problems (Moore, 2002, p.VII- XV). Given that, as mentioned in chapter one, this research is interested in developing a theoretical explanation for the relationship of the cultural affect on both privacy attitudes and perspectives of Internet users, this inquiry is considered to be an example of academic research. Social research projects could be conducted using a quantitative approach, i.e. experiments and surveys or using a qualitative approach, i.e. ethnographies and case studies (Creswell, 2003, pp.13-15) depending on a number of considerations:

ontologically, epistemologically and methodologically, which will be discussed in more detail in this chapter.

This chapter provides a detailed summary of the research methodology options for information systems (IS) studies in order to aid the selection of appropriate research methods for data collection and analysis. The chapter starts with a description of ontological and epistemological considerations for the research by including the three main philosophical paradigms: positivist, interpretive and critical paradigms for the former and the positivist or interpretive for the latter. The chapter then proceeds to describe quantitative and qualitative research strategies, including specific research methods and data collection techniques, such as, the interview, questionnaire, case study and focus group. The chapter then concludes by formulating the proposed research paradigm, methodology, methods, and data collection and analysis strategies and techniques for this research study.

It is useful to establish *from the outset*, a common terminology, especially for the most frequently used terms in this chapter and in future ones. Such terms include methodology, methods, model and concept. It is also worthwhile trying to understand the relationship between theory and research as well as drawing a line of distinction between the quantitative and qualitative research approaches in order to be able to evaluate them in terms of their appropriateness to the aims of this research.

Methodology in social science according to Pawson (2000, p.10) is, "The study of how sociological claims to specialized knowledge of societies are validated."

It is also considered to be, "How we go about studying any phenomena." (Howley, 2007, p.51)

With regard to social research methods, which could be historical reviews and analysis, surveys or field experiments, they are techniques for data collection and it could be defined as, "A systematic and orderly approach taken towards the collection of data so that information can be obtained from those data." (Jankowicz, 1991, p.158)

In other words, method is considered a specific research technique (Silverman, 2005, p. 98). As for models and concepts in social research, "Models provide an overall framework for looking at reality" whereas "concepts are (...) specified ideas deriving from a particular model." (Silverman, 2005, p.98).

3.2 RESEARCH PARADIGM

The description of the relationship between theory and research is not an easy task. Two main issues are associated with such a description. One is the type of theory that would be used by the researcher and the other one is the purpose of the data collection, whether it is to build a new theory or to test an existing one (Bryman, 2008, p. 6).

With regard to the type of theory, there are two forms: deductive and inductive (Figure 3.1). In deductive theory, the researcher's interest lies in an existing theory. They might generate some hypothesis regarding this theory, collect some data, present their findings and finally conclude with hypotheses that either confirms or rejects the investigated theory. This process of deductive theory is the common way of describing the relationship between theory and research within social research. By contrast, with inductive theory, the researcher observes phenomena, generates hypotheses, collects and

analyzes data about these phenomena, presents their findings and finally concludes by generating theory (Bryman, 2008, pp.6-12).

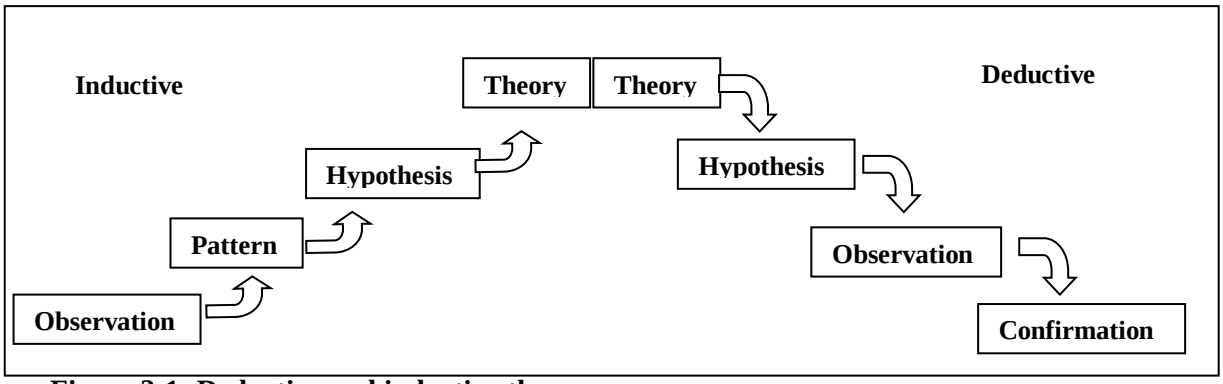


Figure 3-1: Deductive and inductive theory (http://www.socialresearchmethods.net/kb/dedind.php)

Relating to the aim of this research, i.e. studying the relationship between privacy and the Internet and how it is affected by the cultural backgrounds of individuals, the deductive theory is the ideal way to study this phenomena. The process starts by forming a theory, i.e. a research model in this case, based on the literature review of online privacy and its culture affects. This is followed by developing and testing a number of hypotheses in order to confirm or reject all or some of the relationships within the proposed research model.

Regarding the purpose of the data collection, that is, whether it is to test a theory or to build a new one, there are two main considerations when researchers collect data for their research: epistemological and ontological, that is, the basic philosophical paradigms regarding what constitutes knowledge and the nature of reality (Bryman, 2008, pp.13-24). In addition, the philosophical paradigm could be defined as a set of beliefs that provides a view of the nature of the world, the entities within it and their

possible relationships to the world (Guba and Lincoln, 1992). Therefore, the designing of a research investigation requires answering three questions: the ontological question, the epistemological question and the methodological question.

With regard to the ontological question, which interrogates the form and nature of the reality studied, we may ask, for example, what is it? What does it mean to be? How are things really? How do they work? Ontological considerations help social researchers to answer an important question about whether they should study social phenomena taking into consideration the role of the social actors, that is, constructionism or independently, that is, objectivism (Bryman, 2008, pp.13-24).

Regarding the epistemological question, that is, "the principle of knowledge" (Stahl, 2007), researchers try to identify the nature of their relationship with the target data. The epistemological question concerns what is acceptable as knowledge in a particular discipline (Bryman, 2008, p.13).

The epistemological position could be either positivist or interpretive (Oates, 2006, p.282 and Denscombe, 2010, p.226). From a positivist position, knowledge is believed to be gained purely through the gathering of empirical facts and, therefore, the adaptation of natural science methods to the study of social science is fully supported by this position (Bryman, 2008, pp.14-15 and Denscombe, 2010, p.224). Positivism holds that human behaviour can be established and predicted if they have been previously examined in situations similar to those for which the prediction is made (Howley, 2007, p.54).

From the interpretive position, there is a basic distinction between the natural and social sciences, whereby social knowledge is the result of the interaction between people in their society, not just an object that is there to be discovered using positivist methods (Howley, 2007, p.55, and Denscombe, 2010, p.236). Therefore, in interpretive studies, it is recommended that the differences between people and the objects of the natural sciences should be considered in any adaptation of natural science methods to the study of social reality (Bryman, 2008, pp.15-16).

This research intends to look at the relationship between the cultural effects and the online privacy perspective objectively by recording specific attitudes and incidents about the participants regarding online privacy rather than constructing relationships from the participants' explanations. The research also intends to gather empirical facts about the cultural effects upon online privacy attitudes and privacy perspectives rather than study the interaction between the participants and their online environment with regard to their privacy perspectives. This would be done by ranking the level of participants' agreements with a number of statements that describe the variables of this phenomenon (the online privacy attitudes and the online privacy perspective) then looking for any mathematical relationship between these variables.

With regard to the methodological question, which is "the way of obtaining the knowledge" (Stahl, 2007, p.118) the researchers must fit how they are going to find the answer to what they try to study to their ontological and epistemological positions. With respect to epistemological considerations, there are a number of methods associated

with the positivist position, such as, questionnaires, structured interviews and experiments in which all collected data is countable and measurable (Howley, 2007, p.54 and Denscombe, 2010, p.226). Other methods correspond in particular with interpretive considerations, such as, semi- and un-structured interviews, case study and observation from which the collected data provides rich insights for researchers into the area of investigation (Howley, 2007, p. 56 and Denscombe, 2010, p.63).

3.2.1 THE POSITIVIST PARADIGM

Positivist methods are considered to reflect an approach to knowledge that represents a point of view independent of observers from which an account of reality can be objectively given (Stahl 2007, p.118). There are two assumptions behind positivist methods, namely, that the world is not random and that it can be investigated objectively. In other words, the positivist researcher seeks objectively to find regular laws in the investigated area that exist independently of his cognition and experience. This could be achieved by using the principle of deductive theory (Ponterotto, 2005, p.128). The process commences by forming a set of hypotheses that aim to explain reality. These hypotheses are then tested by looking for evidence to prove that they are not false, which would lead to a conclusion that these hypotheses could be true and are representative of reality (Oates, 2005, pp.283-284).

Positivisms share a number of collective characteristics that are shared among positivist researchers. The first characteristic is that the world exists independently of humans, that is, the world in its physical and social forms exists not just in the researchers' minds but also in reality. Thus, since the positivist generally assumes that reality is objectively

given then its measurable properties, which are independent of the observer, that is, the researcher and his or her instruments are able to describe them. The second characteristic is that the world can be studied by conducting observation and using measurement and modelling. Another characteristic is that researchers are studying the world objectively and independently of their personal values and beliefs. The fourth characteristic is that positivism depends on creating hypotheses about the world and testing them empirically, therefore, positivist studies generally attempt to test theory in an attempt to increase the predictive understanding of phenomena (Oates, 2005, pp.283-284). In line with this, information system research could be classified as positivist if there was evidence of formal propositions, quantifiable measures of variables, hypothesis testing and the drawing of inferences about a phenomenon from the sample to a stated population (Orlikowski and Baroudi, 1991, p.50). The fifth characteristic is that the analysis of positivist research data tends to depend heavily on statistics and mathematical analysis and it is considered, therefore, a quantitative data analysis method. The sixth characteristic of positivist research is that the researchers aim for the universal laws, that is, generalizations, which could be proven true regardless of their knowledge.

The quality of positivist research is judged by four criteria: objectivity, that is, freedom from research bias; the reliability and accuracy of the research instruments; internal validity, for example, with regard to examining and collecting appropriate variables and data; and external validity, for example, selecting a representative sample (Oates, 2005, pp.283-284).

3.2.2 THE INTERPRETIVE PARADIGM

Interpretive methods are considered a social construction on the part of human actors who believe that their knowledge of reality is a part and product of human actions. The use of interpretivism in IS research has become more commonplace compared with the situation in the 1990s (Walsham, 2006, p.320). The use of interpretive studies is controlled by particular guidelines including choosing the style of involvement, gaining and maintaining access, collecting the data and working with different countries (Table 3.1), (Walsham, 2006, pp.320-330).

Table 3-1: Guidelines for carrying out interpretive studies

Setting up activities	Guidelines
Choosing the style of involvement	**Outsider researcher: using formal interviews** **Involved researcher: using observation techniques**
Gaining and maintaining access	**Good social skills / Persistently trying alternative options / Providing feedback**
Collecting the data	**Timekeeping during the interview /Balance between passivity and over-direction / Confidentiality / Audio-recorded**
Working with different countries	**Aware of the different cultures** **Study the history and the culture of the target countries**

Interpretive researchers start out with the assumption that access to given or socially constructed reality is only through its social constructions, such as language, consciousness and shared meanings. The philosophical basis of interpretive research is hermeneutics and phenomenology (Boland, 1985). Interpretive studies generally

attempt to understand phenomena through the meanings that people assign to them. Interpretive methods of research in IS are, "Aimed at producing an understanding of the context of the information system and the process whereby the information system influences and is influenced by the context." (Walsham, 1993, pp.4-5). Interpretive research does not predefine dependent and independent variables but focuses on the full complexity of human sense making as the situation emerges (Kaplan and Maxwell, 1994).

Similar to the positivism, interpretivism methods also share a number of characteristics. The first characteristic is that there are multiple subjective realities, that is, there is no one reality and knowledge is a creation of the researcher's mind. The second characteristic is that reality can be described to others by socially constructed means, such as, language or its shared meanings. Another characteristic of interpretivism is that the researchers' values and beliefs play a role in shaping the research process. The fourth characteristic is that interpretivist research studies people in their natural social settings not in an artificially constructed experimental world. The fifth characteristic is that the analysis of interpretivist research data tends to depend on qualitative data analysis methods. The sixth characteristic of interpretivist research is that researchers should not produce a rigid description of phenomena; instead, they are expected to construct open multiple interpretations of phenomena (Oates, 2005, pp.292-293).

3.2.3 THE CRITICAL PARADIGM

As with interpretivism, the critical research paradigm proposes that social reality is a consequence of the researcher's understanding of the world. Critical researchers, however, extend their enquiry to include an investigation into why a specific way of understanding the world tends to dominate the way of seeing reality (Oates, 2005, pp.296-300). In addition, critical researchers believe that social reality is historically produced, shaped and reproduced by people (Orlikowski and Baroudi, 1991, p.19; Ponterotto, 2005, pp.129-130).

Critical researchers are interested in identifying the power relationships within social constructions and empowering people to eliminate any conflicts (Ponterotto, 2005, pp.129-130; Oates, 2005, pp.296-300). In other words, critical researchers are concerned with disagreement and challenge existing society in order to eliminate the causes of the disagreement (Ponterotto, 2005, pp.129-130).

3.2.4 SELECTED PARADIGM

Based on epistemological and ontological considerations, that is, the philosophical paradigms that were described earlier, it can be argued that the nature of a social research study has an effect on the selection of the appropriate research paradigm (Bryman, 2008, pp.13-24). This research investigates the relationship between online privacy perspectives and the cultural background of individuals and uses a deductive theoretical approach (Ponterotto, 2005, p.128). Deductive theory is based on hypotheses concerning relationships between variables, such as, the online privacy perspective and certain cultural characteristics of individuals, in order to describe an account of reality

and then test these hypotheses by looking for evidence that will prove that these relationships are not false. Thus, the conclusion can be drawn either that these hypotheses are a true representation of reality or that they are not (Oates, 2005, pp.283-284). Therefore, it can be argued that the positivist paradigm is the appropriate choice of research paradigm for this study.

3.3 RESEARCH METHODOLOGIES IN IS RESEARCH

Disciplined inquiry in IS research could be divided into quantitative and qualitative inquiry (Figure 3.2). Quantitative research is described as a research strategy that underlines quantification in the collection and analysis of data in order to understand a phenomenon or test a theory particularly in a way to show "what is happening." By contrast, qualitative research is described as the use of research to understand phenomena or test a theory using a research strategy that usually stresses words rather than numbers in the collection and analysis of data in a way to determine "Why it is happening" (Bryman, 2008, pp.21-23 and Moore, 2002, p.121).

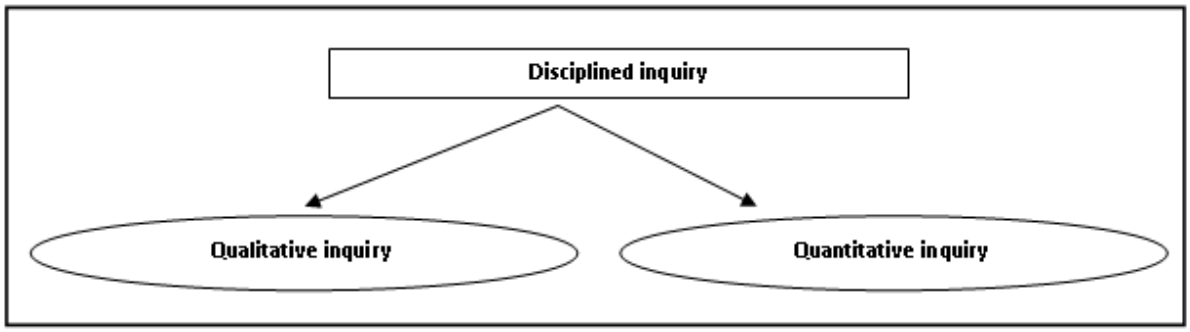


Figure 3-2: Conventional Disciplined Inquiry

Nevertheless, this conventional model of disciplined inquiry through two distant approaches to research is not helpful in distinguishing between qualitative and quantitative approaches in social science; therefore another disciplined inquiry model

has been suggested (Figure 3.3) in which the distinctions between the four aspects of the research process, that is, paradigm, strategies, method and analysis are considered (Hill, 1999).

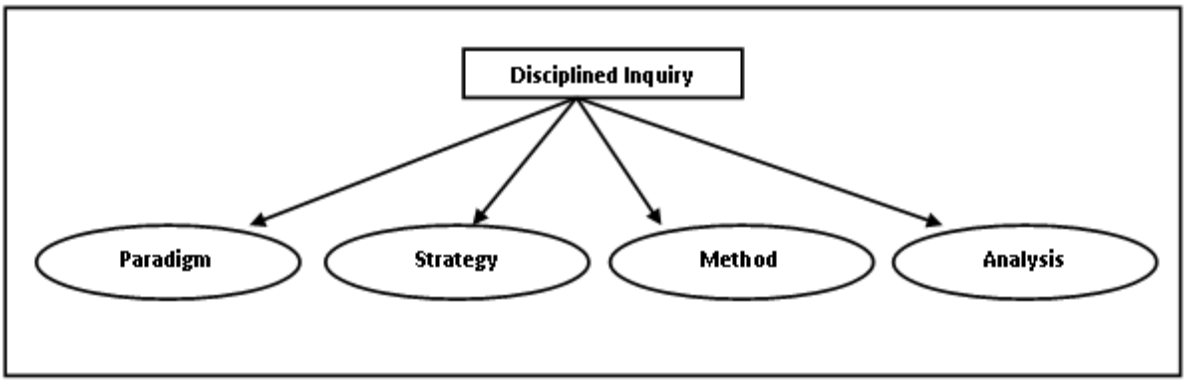


Figure 3-3: Alternative Model of Disciplined Inquiry

Quantitative research methods, their types, advantages and disadvantages will be described in section 3.3.1 while qualitative research methods, their types and relevance will be described in section 3.3.2.

3.3.1 QUANTITATIVE RESEARCH

Quantitative research is interested in numeric evidence that could be observed by looking for patterns in the data (Oates, 2005, p.210). The quantitative research strategy represents a deductive view of the relationship between theory and research in which the philosophical paradigm is that of positivism (Bryman, 2008, p.140). In quantitative research, the data collected from the targeted participants is counted and collated to present them as measurable and classified data. This can therefore lead to the building of an objective hypothesis about such phenomena (Howley, 2007, p.51). Denscombe (2010, p.269) states that the quantitative approach has attracted researchers on the grounds of its scientific propriety. The author argues that the reason for this popularity

is the use of numbers and their association with graphs and tables that present the findings.

In the context of this research, the survey method will be used for quantitative research. Some researchers consider surveys as part of a group of methods that emphasize quantitative analysis, such as, the questionnaire and structured interview (Gable, 1994, p.113). The questionnaire as the main data collection method of this research will be reviewed briefly in this chapter and in more detail in Chapter Five.

3.3.2 QUALITATIVE RESEARCH

Sometimes it is not easy to understand numerical data and therefore detailed and meaningful insights are needed in order to interpret it (Howley, 2007, p.52). A qualitative research strategy is required for a task that underlines words rather than numbers in both its data collection and analysis phases. The qualitative research strategy represents the inductive view of the relationship between theory and research for which the philosophical paradigm is interpretivism (Bryman, 2008, pp.366-370). Although qualitative research includes a number of techniques, they have in fact common elements, such as, a concern with meaning and the way people understand things as well as with patterns of behaviour rather than their frequency (Denscombe, 2010).

Later in this chapter (Section 3.4.2), the case study as a qualitative research strategy will be discussed in more detail. The reason for this decision is that the research strategy of the case study covers a number of methods, such as, participant observation and in-depth semi-structured interviews (Gable, 1994, p.113). Focus group interviews will also

be discussed briefly in this chapter as well as in Chapter 4 as part of the data collection strategy selected for this study.

3.4 RESEARCH METHODS AND RESEARCH DESIGN

A research method is a data collection technique that implies the use of a specific instrument, such as, a survey, an interview and observation, through which the researcher collects data from the research subjects, that is, the participants. The research design, on the other hand, provides a framework for data collection and analysis. It can be constructed to study the causal connection between variables, to understand social behaviors and their meanings in a social context and can enable the researcher to generalize their findings to include larger groups of individuals (Bryman, 2008, p.31).

In this section the main research methods available, such as, the survey (i.e. questionnaire and the structured interview), the semi-structured interview, the case study and the focus group interview will be briefly described. Qualitative and quantitative data analysis frameworks will also be explained in this section.

3.4.1 SURVEY

A survey is a specific approach used to collect social data. It involves the collection of the same data from all cases in a sample of participants, each possibly with different motivations and backgrounds. The term ‘survey’ embraces a group of methods including questionnaires and interviews, particularly large-scale structured interviews, amenable to quantitative analysis of the data collected using statistical techniques (Denscombe, 2010, pp.11-12; David and Sutton, 2004).

In addition, the aim of a survey is to discover and, therefore, establish common relationships across a group of participants and so be able to produce a generalized statement about the phenomena investigated. It is a research strategy rather than a research method. There is a multitude of surveys. They include questionnaires, structured interviews, documents and observation (Denscombe, 2010, pp.11-19). In this chapter, questionnaires and structured interviews will be briefly described. Questionnaire design and analysis will be discussed in more detail in Chapter 5.

Survey usage is associated with a number of advantages including the collection of wide and inclusive coverage of empirical data that is easily measured and, therefore, can be generalized (Denscombe, 2010, pp.48-49). There is, however, a number of drawbacks to using surveys including the problem of the low response rates. The target participants can relate using questionnaires to inaccurate or dishonest responses, which will be mostly undetectable by the researchers (Gable, 1994, p.113, and Denscombe, 2010, p.48-50).

3.4.1.1 Questionnaires

A questionnaire is a pre-defined, prearranged and self-administrated set of questions that is designed by the researcher to collect brief and uncontroversial data from a large number of targeted participants (Oates, 2005, p.219). A postal questionnaire is a popular type of survey. It is conducted through designing self-completion questionnaires about the investigated phenomena and then posting them to the addresses of an appropriate sample of key people, *that is, participants*, within a wide geographical area (Denscombe, 2010, pp.155-156). The author identified a number of research situations that would make questionnaires the appropriate type of survey. One situation is when

the research requires information from a large number of participants from a wide geographic area with a relatively flexible time for production, piloting, posting and collecting the questionnaires and then analysing the data (Denscombe, 2010, pp.155-156).

In order to understand the process of how the participants are answering a questionnaire the questionnaire designer could use cognitive theory (Tourangeau, 1984, pp.299-314, Tourangeau, and Rasinski, K., 1988, Dou *et al.*, 2010, p.265, Ziegler, 2011, p.30). This will enable the designer to validate and test the questionnaire and ensure it is fit for purpose. Under the proposed cognitive theory, respondents would go through four stages when responding to questionnaire items. At the first stage, the respondents start to comprehend the question, that is, to understand the question's intention and the meaning of its terms, specific words and phrases. Then the respondents start retrieving the relevant information from their memory. This would include identifying what information is needed and what recall strategy is required, for example, do they need to count or estimate.

At the third stage, the respondents enter the decision processes of their response and decide whether they will answer the question. This would depend heavily on whether they have the motivation to respond, that is, whether they can muster adequate intellectual effort and whether they want to tell the truth, which relates to the sensitivity or liability of the question. Finally, the respondents enter the response process stage in which they try to match their own response to the response options given by the questionnaire (Willis *et al*, 1999, pp.2-3).

Researchers who use questionnaires are advised to provide a written cover letter enabling informed consent with the questionnaires that includes details of the aim and process of the research, as well as an explanation of the mechanism for storing, accessing and discarding the collected data (Oliver, 2003, pp.56-58). Respondents can also be reminded that they do not have to answer any question that they consider inappropriate for them and they do not have to include their names with the questionnaire response. Such practices, that is, enabling informed consent, outlining the participants' rights and ensuring that responses are voluntary and confidential are very important as moral objectives and also to build trust among the participants for any future research (Bryman, 2008, pp.118-128). Although, the voluntary principle conflicts with the representative sampling one and could create or increase sampling bias, compulsory participation should be not an option. The solution to issues of sampling bias due to non- representative sampling could be solved statistically, such as, weighting (Vaus, 2002, pp.59-60).

3.4.1.2 Structured interview

In the structured interview the level of control over the format of questions and their answers is similar to that for questionnaires in that they comprise of a list of questions in face-to-face administration and are, "In an ordered style with limited words for answers, which are carried out in person".

The reason behind selecting the structured interview is to create standardization. Here the participants are presented with identical questions and a range of pre-coded answers and, therefore, provide quantitative data that is relatively easily analyzed using statistical methods (Denscombe, 2010, pp.174-175). Although the structured interview

is considered to be a quantitative research strategy (Section 3.4.1.2) it is essential to emphasize that some forms of the interview are qualitative in nature. This is particularly true of semi-structured and unstructured interviews (Section 3.4.3) in which the data are collected on a small scale and analyzed with more insight and in much more detail (Gable, 1994, p.113).

Interviews could be classified according to their method of administration, for example, face-to-face, telephone and internet interviews. In face-to-face interviews, the more popular form of interview, questions are asked and answered with direct contact between the researcher and the respondents. In this case, the response rate would in fact be arguably higher than that of other survey types. Interviewees would be carefully selected according to their gender, age and cultural backgrounds (Denscombe, 2010, pp.16-17).

The telephone interview is popular in social research. Denscombe (2010, pp.14-15) and Bryman (2008, pp.197-199) argue that there are many reasons for this popularity. One of these is the savings in cost and time that can be made with this method compared to face-to -face interviews where the researcher has meet each interviewee's travel costs. Another reason according to Denscombe (2003, pp.9-10) and Bryman, (2008, pp.197-199) is that there is evidence that people are more honest and open in telephone interviews compared to face-to-face interviews.

3.4.1.3 Online Survey

The use of the online survey has become popular with increased use of the Internet and of computer-mediated communication technology (Cobanoglu, Warde and Moreo,

2001, p.405, and Wright, 2004, p.239). The use of online surveys has a number of potential advantages over the mail and telephone survey, for example, researchers who are using online questionnaires can get access to target participants in distant locations within a short period of time and at a low cost. Online surveys, however, may create concerns over sampling procedure and uncertainty about the validity of the collected data. The sampling issues could be, for example, the existence of multiple e-mail addresses for one participant or invalid/ inactive e-mail addresses for others, which create problems for the random sampling technique.

3.4.1.4 Sampling in survey research

It is difficult, if not impossible, to collect data from everyone in the category investigated. Alternatively, data could be collected from a portion, a sample, which represents the whole population of this targeted category. It is necessary to select a sampling approach that may be carefully applied to the population (Denscombe, 2010, p.23).

Within social research, two sampling techniques ensure a representative sample of the population. One technique is 'probability sampling' whereby the researcher seeks indications that the selected sample may be representative of a range of members of the entire targeted population. The other technique is 'non-probability sampling' in which the researcher decides to conduct sampling without knowing whether the selected sample may be representative of the entire targeted population.

According to the nature and feasibility of the conducted research there are five types of probability sampling techniques, namely, random, systematic, stratified, cluster and

multi-stage sampling. In random sampling individual members (units) of the sample frame, which could be drawn from a telephone or e-mail directory, would be randomly selected (David and Sutton, 2004, pp.149-151 and Denscombe, 2010, pp.24-38). Each member of the targeted population, therefore, would have the same chance of being selected (Bryman, 2001, p.88) whereas in systematic sampling only the first in the sample is selected randomly and the rest of the sample is selected using a system, such as, every '*n*th' number (Denscombe, 2010, p.28).

Stratified sampling is similar to random sampling in that each member of the population has the same chance of being selected. The selection, however, takes place within representative strata, such as, gender, age or the geographic area of the population. In cluster sampling, groups from the population, that is, from a particular geographic area are selected according to convenience, resources and time and a random sampling technique is applied to this group. In multi-stage sampling the selection of both the cluster and its members are random (Denscombe, 2010, pp.29-33).

The non-probability sampling technique is used only if there are impractical barriers in applying the probability sampling technique, for example, if the actual number of the targeted population is not known or if some of the population's members were not accessible due to age, sex or political restriction and, therefore, they would be excluded from the selected sample. As a result, this sample cannot be categorized as probability sampling. There are four types of non-probability techniques: purposive sampling, snowball sampling, theoretical sampling and convenience sampling (Denscombe, 2010, pp.34-38 and David and Sutton, 2004, pp.151-152).

In order to realise a successful sampling technique researchers are required to use a proper sampling frame as well as taking into account a number of issues, such as, the sample frame and its size and an acceptable response rate. With regard to the sampling frame, it must be relevant and linked directly to the research topic with complete, precise and up-to-date specifications (Denscombe, 2010, pp.34-38).

The pursuit of a balance between group or cluster samples and sampling the entire population aims to prevent non-representative samples. Obtaining a representative sample is very important to enable the generalisation of the findings to the whole population (Denscombe, 2010, p.29).

The size of the representative population sample is also a crucial factor when the findings of a survey are to be generalised and in general, a big sample size is better. Nevertheless Bryman, (2001, p.93) claims that there is no one definitive answer to the question of sample size, which depends on a number of factors, such as, time, cost and response rate.

Another important issue that is associated with the sampling technique is the response rate, which is described by Bryman, (2001, p.93) as the percentage of the selected participants who agree to participate. The author illustrates how to calculate such a response rate in which the number of usable questionnaires is divided by the number of suitable members of the sample and multiplied by a hundred. In addition, Denscombe (2010, pp.40-42) insists that the main problem that can face any sampling technique, sampling bias, can result from a poor response rate. Therefore, it is advisable to predict

the likely response rate in advance, which in fact is based on experience and personal judgement rather than any mathematical formulation.

3.4.2 CASE STUDY

The aim of the case study is to understand the problem being investigated with an opportunity to ask insightful questions to answers, which, however, may not be possible to generalize.

There are two reasons for selecting an appropriate case study. These are either the suitability or the practicality of such a case study (Denscombe, 2010, pp.58-60). Regarding suitability, in order to have a good and convincing case study that meets the purposes of our research, we need to carefully select the case and justify our selection (Payne *et al.*, 2007, p.243). The suitability test is generally based on four criteria: typical instance, extreme instance, test-site for theory and least likely instance. A typical instance, the most common type of case study, could aid the generalization of any findings, as it would be similar to those selected and examined by other researchers in the same field. An extreme instance would serve as a contrast to the standard or typical instance (Payne *et al.*, 2007, p.244 and Denscombe, 2010, pp.34-38).

In addition, a case study could serve as a test site, that is, for theory testing rather than theory building whereby the researcher would predict a certain outcome from a case study according to an existing theory in order to prove this premise. The fourth type of case study, the least likely scenario, to some extent is similar to the third type of case study or test site. The former would be used in order to test a particular theory by trying

to prove it true in the least expected circumstances. If the theory can be applied in this least expected situation, the theory would be proven (Darke, Shanks and Broadbent, 1998, p.275).

With regard to practicality, the justification for the selection of a case study is sometimes based purely on pragmatic motivations. Here the case is selected because it is a matter of convenience or because it is intrinsically interesting (Seawright and Gerring, 2008, pp.295-296).

There are three dimensions of the case study's strength that commend it as a social research methodology for IS. One is that information systems can be studied in a natural setting where the state of the targeted phenomena can be learned and, therefore, theories can be generated from practice. The strength of the case study also comes from its nature and the complexity of its process within the studied phenomena, which allows a deep understanding of the phenomena that are under study. The third aspect of the strength of the case study is the emergence of valuable insights into new topics in the field of rapidly changing information systems (Benbasat *et al.*, 1987, p.370).

There are a number of weaknesses associated with the use of case studies as a research strategy. First is the inability to manipulate independent variables within a case study. Second is the risk of improper interpretation of the phenomena. Third is the lack of power to randomize the source of data for these phenomena (Kerlinger, 1986, p.348). Other weaknesses are the lack of controllability, deductibility, repeatability and generalisability (Lee, 1989). Bryman (2008, p.57), however, argues that the purpose of

using a case study is not to generalize findings; instead it tends to provide a rigorous understanding of a single case. Bryman adds that researchers could generalize their case study's findings by comparing their cases to others.

3.4.2.1 Semi–structured and unstructured interviews

In semi-structured interviews, the order of questions is flexible in order to give the interviewee the opportunity to speak freely about the investigated issue and, therefore, enhances the discussion with deep insights into the topic. The unstructured interview allows further freedom, enabling interviewees to develop their ideas regarding the topic being investigated without a strict format. Both types of interview are used mainly in qualitative research. Similarly, to structured interviews, semi-structured and unstructured interviews could be classified according to their mode of administration, for example, face-to-face, telephone and internet interviews.

The most complex interactive moment between the researcher and participants is during the interview itself where a number of important issues occur (Oliver, 2003, pp.45-56). For example, it is possible that just before the interview the interviewee asks for more details about the research or a copy of the collected data or hesitates about co-operating for a number of reasons, particularly if the semi-structured or unstructured interview is to be recorded or videoed instead of being recorded by hand written notes. Therefore, full information on the research investigation and the process of obtaining, storing, accessing and discarding the collected data must be offered to interviewees in advance (Oliver, 2003, pp.45-56).

Regarding the tape or videotape of the interview, some interviewees could be intimidated by this, thus preventing them from expressing their views regarding sensitive matters that might arise during the interview, perhaps because their identity might be revealed accidentally by saying their name during the recording. In order to minimize the intimidation and to ensure that interviewees feel comfortable a number of strategies specifically regarding their anonymity could be adopted. One strategy is to place the digital recorder within easy reach of interviewees and tell them that they can press the record button or even stop the session if they feel they want to do so. Another strategy is to offer to play back the recording to the interviewees to ensure that what they said represents their true feelings regarding the issues discussed and the opportunity to erase any part they want to exclude from the interview (Oliver, 2003, pp.45-56).

3.4.3 FOCUS GROUP

The focus group is a research technique for collecting data using group interaction, that is, several participants in addition to a facilitator on a targeted topic and specific issue (Bryman, 2008, pp.473-476). Bryman argues that the focus group is different to the group interview in that the former tends to investigate an explicit topic in depth rather than covering a broad issue. A focus group is interested in individuals' points view with regard to the topic. He adds that using a focus group allows the researcher to develop a fuller explanation of people's views not by only asking them directly but also by allowing them to probe and challenge each other's views. Such behaviour would be difficult to record by the interviewers themselves in one-to-one or group interviews.

Morgan (1996, p.139) argued that focus groups provide not just output data from the participants but beyond this to include an insight into certain their complex behaviours and motivations and, therefore, their output. This happens only because of the interaction between focus group participants and it is called the group effect. In addition, focus groups provide an instant comparison due the actions of the participants themselves within the group rather than through the researcher via individual interviews.

Morgan (1996, pp.134-136) argues that focus groups and surveys are the main ways of combining qualitative and quantitative methods. He outlines four ways of combining them in using these techniques, which are presented in Table 3.2. In the first strategy, which is mainly used by market researchers and relatively recently by social researchers, the research begins with the focus groups as an initial phase to study how the respondents counter and discuss the targeted topic of the research. The researcher is then able to use this information to design the questions for a survey, which is eventually used as the primary method. In the second strategy, which is more relevant in medical research, the inquiry is initiated by surveys in order to help the researcher select the most relevant samples for their focus groups, which is used as the primary research method (Morgan, 1996, pp.134-135).

In the third strategy, both focus groups and surveys are conducted. The surveys, similar to the first situation, are applied as the primary (quantitative) research method while the focus groups (qualitative) are used as a follow-up research method to clarify poorly understood data from the survey's results. In the fourth strategy, focus groups are used

as the primary research method and followed up by surveys to collect secondary data that aims to examine statistically the frequency of issues or themes from the focus group (Morgan, 1996, p.135).

Table 3-2: Situations of combining focus groups and surveys

	Surveys	Focus Groups	Relevant Situations
1.	Primary Method	Initial Method	Mostly in market research and in some new social research
2.	Initial Method	Primary Method	Mostly medical research
3.	Primary Method	Follow-up Data	Clarifies poorly understood data from the results of the surveys
4.	Follow-up Data	Primary Method	Examines the frequency of issues or themes from the focus group

Based on the discussion above and as can be seen from Table 3.2 in this study the focus group method will be used as an initial phase to study how the target participants respond to and discuss the relationships between online privacy perspectives and the cultural background of Internet users. Therefore, a number of focus groups will be conducted and analysed in preparation for the main data collection method, that is, the questionnaire. Morgan (1996, pp.134-135) supports this combination of focus group and survey in social research.

3.5 SELECTED RESEARCH PARADIGMS, AND RESEARCH METHODOLOGY

This research will have a prescribed plan for collecting and analysing quantifiable measures of its main variables, that is, online privacy perspectives and cultural

background, testing hypotheses about relationships between these variables and drawing conclusions about the relationships between phenomena from a selected sample of the target population. It, therefore, could be argued that this research uses the assumptions of the positivist paradigm in its investigations (Orlikowski and Baroudi, 1991, p.50). It also represents the positivist research paradigm, as discussed above (Section: 3.3.1) due to the deductive view of the relationship between theory and research (Bryman, 2008, p.140). Consequently, quantitative research is the most appropriate research methodology for the selected paradigm.

In addition, the aim of this research is to determine relationships between the online privacy perspectives and the cultural background of Malaysian and Saudi Arabian Internet users and to be able to produce a generalized statement about different influences on the online privacy perspectives of the target population. Such aims, according to Denscombe (2010, pp.26-27), can be achieved through a survey strategy, in particular, a questionnaire. The questionnaire survey enables the researcher to gain a wide coverage of empirical data that are easily measured and can be generalized (Denscombe 2010, p.49).

3.5.1 DATA COLLECTION

Data collection is divided into two main stages: initial data collection and main data collection. During initial data collection stage a number of focus groups were conducted in order to aid the preparation for the main data collection (Morgan, 1996, pp.134-136) by gathering primary data on individual online privacy perspectives and the impact of their culture in shaping them. As a result, a research model was design from the primary

data as well as the from the literature review. More details about the first stage are described in chapter four.

During the main data collection stage a self-completion questionnaire survey was used to gather data on a number of constructs that were driven from the research model and its hypothesis. In addition, the items or questions that formed the constructs were selected from validated items from relevant literature about Internet privacy concerns. Before collecting the data two pilot tests were conducted. First test, the questionnaire's validity, ensured that the questionnaire items would measure the relevant concepts they were intended to measure (Ruane, 2005, pp.32-42, and Sarantakos 2005, pp.254-256). The second test, the questionnaire's reliability, ensured that participants would answer the questions in the same way every time the questions were asked (Vaus, 2002, pp.52-54, Bryman, 2008, pp.149-154). More details on the questionnaire's design and validation are provided in chapter five.

3.5.2 DATA ANALYSIS

Data analysis, for the main data, i.e. the questionnaire, was divided into two stages. First, a contingency analysis, to examine the affect of nationality, gender and age groups on the online privacy perspectives of the participants by using contingency tables and chi-square tests of independence (Field, 2009, p.688 and p.783 and Howell, 2010, p.15-148). Second, a simple linear regression analyses to test the research model's hypotheses, by measuring the Pearson Correlation Coefficients (r), (Field, 2009, p204, and Pallant, 2007, pp.166-178), Independent Samples T-tests (t) and ANOVA and P-values (p) on the samples (Field, 2009, pp.334-341, and Pallant, 2007, pp.232-265).

Prior to conducting the above mentioned data analysis test, the data was screened for accuracy, outliers within cases (Tabachnick and Fidell, 2007, p.60) and normality (Hair *et al.*, 1998, pp.71-73, Tabachnick and Fidell, 2007, p.79 and Field, 2009, pp.155-156). More details on the data screening and analysis are described in chapter six.

3.6 CONCLUSION

The aim of this chapter was to provide a basis for a decision to be made about appropriate research methods for data collection and analysis for this study by reviewing the research methodology options for IS studies. The discussion in this chapter included a description of the ontological and epistemological considerations for the research and of the three main philosophical paradigms: the positivist, interpretive and critical paradigms. The discussion contains an account of quantitative and qualitative research strategies and some of the associated research methods and data collection techniques, such as, the interview, questionnaire, case study and focus group. The chapter concluded with the selection of the positivist paradigm and a quantitative methodology using the questionnaire survey method for data collection, analysis strategies and techniques for this research.

At the following chapter, the designing, conducting and the finding of focus groups, would be discussed in details. Focus groups is considered as a part of the methodology of this research and used as an initial data collection to aid the designing of the primary research instrument, the questionnaire survey.

4 CHAPTER 4: INITIAL DATA COLLECTION: FOCUS GROUPS

4.1 INTRODUCTION

Chapter 3, the research methodology, described the ontological and epistemological considerations and the three main philosophical paradigms (positivist, interpretive and critical) relevant to this research. In addition, the chapter also covered quantitative and qualitative research strategies, research methods and data collection techniques, such as, the interview, questionnaire, case study and focus group.

As it has been mentioned in chapter one, the aim of this research is to explore the relationship between online privacy perspectives and Internet users' cultural background, which includes the Internet users' social norms, religious beliefs, the Internet regulations in their country, their IT skills, nationality and gender and how it is affected by the cultural backgrounds of individuals in Islamic cultures. To accomplish this academic aim, a research methodology was designed to collect the target data in two main stages: initial data collection using focus groups and main data collection using questionnaire survey. The initial data collection stage which includes a number of focus groups would be described in this chapter.

As mentioned in Chapter 3, the focus group is a research technique for collecting data using group interaction on a targeted topic and specific issue. It involves several participants in addition to a facilitator (Bryman, 2010, pp.352-358). The focus group, as mentioned above, is part of the methodology of this research, which is used to prepare the way for the primary investigative instrument, questionnaire survey. This chapter is

divided into six sections. The first section involves a brief comparison between focus groups, surveys and individual interviews and the four possible situations in which focus groups and surveys can be combined. In the second section, certain issues associated with using focus groups as a social research method including standardisation, sampling, group size and numbers of groups are highlighted. In the third and fourth sections, the use of focus groups as a social research strategy to investigate the study's research question and its planning strategy are discussed. Finally, the fifth and sixth sections outline and analyse the main outcomes of the focus groups.

4.2 FOCUS GROUPS AND OTHER DATA GATHERING TECHNIQUES

A number of studies have compared focus groups with other research methods, particularly surveys and individual interviews. These comparative studies were carried out for two reasons. One was to compare the quality of the data collected by the two methods under comparison. Focus groups were found to be most useful when they reproduce results obtained using standard research methods. Another reason was to establish any unique contributions that the focus group method could provide to the targeted research area. The focus group method was found to be very useful in producing new results that are difficult to elicit through other standard research methods (Morgan, 1996, p.136). To complete this section, we present a comparison of focus groups with the survey and individual interview.

4.2.1 COMPARISON OF FOCUS GROUPS AND SURVEYS

In a systematic investigation that compared three studies that used surveys and focus groups it was found 30% of the 60 variables were similar while only 12% were dissimilar (Ward *et al.*, 1991 cited in Morgan, 1996, p.136). The rest of the variables were found to exhibit some similarly with focus groups giving more information than the surveys in 42% of the cases compared to surveys, which only gave more information in 17% of the cases. The researchers concluded that focus groups provided more in-depth information on the area studied. In another systematic comparison of two medical studies (Saint-Germain *et al.*, 1993, cited in Morgan, 1996, pp.137), the findings of both surveys and focus groups were in most cases found to be similar with more information obtained from the focus groups.

4.2.2 COMPARISON OF FOCUS GROUPS AND INDIVIDUAL INTERVIEWS

In an investigation, it was found that each participant in a focus group produced only 60% to 70% of the ideas that they would have produced if they had been interviewed individually (Fern, 1982 cited in Morgan, 1996, p.138). Participants, however, from focus group interviews tend to provide the same contribution to the research topic when they are interviewed individually whereas participants who are (initially) interviewed individually are most likely to give extra or different information when they are recruited later to a focus group interview (Wight, 1994, in Morgan, 1996, p.138). This finding suggests that one of the strengths of focus groups, as outlined in the next subsection, is the influence of the interaction between participants within their focus groups, which can result in providing more output data compared to the sum of the output data from participants in all of the individual interviews.

4.3 PLANNING FOCUS GROUPS

In order to follow the method for using focus groups as set out by Morgan, there will be four main steps: planning, recruiting, moderating and analysing the outcome and reporting the findings (Morgan, 1998, pp.23-31 and pp.131-132).

With regard to planning the expected outcomes, the number of groups, the number of participants per group, characteristics of the participants, budget, timelines and facilities (room, refreshments, stimulus materials, for example, scenarios and questions and audio recordings) need to be defined. Regarding recruitment, the appropriate composition for each group needs to be identified. Meanwhile a specific criterion for individual participants needs to be developed. Studies show that to recruit participants to form a group of eight can take up to 32 calls or visits before enough willing participants are found to be available (Morgan, 1998, pp.23-31). A moderator can then be recruited or alternatively the researcher undertakes the moderation. The moderator's role is set and the materials that they are to use with the focus groups are prepared. With regard to analysis and reporting, an analysis plan is designed to specify elements for the survey. The approach used to analyse the data will be categorising quotations from the focus groups into types of description, i.e. concepts, which are then compared against targeted concepts of privacy perspectives (Kitzinger, 1995, p.301). The following four steps outline the plan for the focus groups.

4.3.1 PLANNING FOCUS GROUPS

The aim of the focus groups are to gather initial data which aids the design of the main data collection technique i.e. questionnaire survey. The outcome of these initial data gatherings together the literature review are expected to help the researcher to identify the research's variables, model and hypothesis. A summary of the expected outcome information from the focus groups is described as follows.

First: Perspective of the individual towards the concept of online personal information

As has been mentioned in the literature review, the type of the personal information that is provided could play a role in the level of privacy concerns and, therefore, upon Internet activities (Smith *et al.*, 1996, p.189 and Dinev and Hart, 2003, p.6). The types of personal information have been discussed in chapter two (Guarda and Zannone, 2008, p.7 and Ghani and Sidek, 2009, p.411). The purpose of first question for the focus group is to explore the participants' points of view on what could be considered personal information.

Question 1: Which of the following personal information matters when you try to protect your right to privacy: your name, home address, phone number, mobile phone number, e-mail address, income, religious views and political views?

Second: Perspective of the individual towards the concept of online privacy

As mentioned in chapter two, a number of individual perspectives lead to the perception of the importance of privacy. They can be philosophical, psychological, sociological,

economical or political (Clarke, 2006, pp.1-2; Kemp and Moore, 2007, pp.58-77). The second question for the focus group is to identify the main perspectives that form the perception of the importance of privacy.

Question 2: Have you experienced a situation where you felt that your privacy or the privacy of somebody you know has been violated in some way? If yes, could you briefly explain what happened and why you felt it violated the right to privacy?

Third: The level of the privacy practice among the participants

The scale for measuring privacy, as mentioned in chapter 2 (Margulis, 2003, p.413), consists of six dimensions: level of the solitude (the level of freedom from others' surveillance) intimacy (the ability to form a closed, relaxed and frank relationship group) anonymity (the freedom from being identified in a public place and for public acts) reserve (the ability to limit disclosure to others) seclusion (the visual and auditory privacy of the home) not neighbouring (not having anyone who would drop in without any warning)

Questions three, four, five and six examine some of the scale for measuring privacy among the participants.

Question 3: Ahmad looks at the chat files on his personal computer, which include all the Microsoft Messenger chats that his wife had with her sisters and friend. He enjoys reading what they say about their husbands, kids and friends, with no intention whatsoever to use, disclose or even mention this very ordinary information to his wife

or anyone else. In this case or similar ones, do you think that Ahmad violated his wife's right to privacy?

Question 4: Samer worries about recent changes in his teenage son's behaviour as he spends all his time either online or outside the home. After many failed attempts to understand what is wrong with his son, for example, by asking him and by talking to his companions, Samer has decided to ask his friend, who is a computer technician, to help him to break into his son's laptop. Do you think that Samer has the right to breach his son's right to privacy? Why?

Question 5: Abdullah studies at a college outside of his city. He enjoys communicating with his family back home using Microsoft Messenger. One day he added a web camera to his PC in order to be able to see his family but his sister Eman refused to appear on the camera. Do you think that this is a common practice within your family and friends? Why?

Question 6: In a place like prison, the prisoners are observed all the time by the guards who at the same time restrict others from any informational and physical access to these prisoners. Do you think that we could claim that these prisoners have privacy? Why?

Fourth: Factors that could affect the individual's perspective on privacy

The seventh question for the focus group is to identify the factors that could preserve online privacy and, therefore, affect the participants' perspectives of their Internet privacy concerns.

Question 7: Do you think privacy can be maintained? What do you think can maintain the right to privacy: the law and regulation, religious background or the development of information technology?

Fifth: Similarities and differences between the perspectives of individuals from different cultures, genders and educational backgrounds towards privacy in internet usage

The cultural backgrounds, i.e. nationality, could affect Internet privacy concerns (Siala *et al*., 2004, p.7). The relationship between gender and Internet privacy concerns, as mentioned in chapter 2, have been studied by a number of researches (Slovic *et al*., 1997, Bartel-Sheehan, 1999, and Kehoe et al from Garbarino and Strabilevitz, 2004, and Liebermann and Stashevsky, 2002). Educational level, according to Liebermann and Stashevsky (2002, pp.297-298), plays a role in the individual's Internet privacy concerns. The effect of a participant's nationality, gender and their level of education are examined throughout the six focus group questions.

There are two extreme suggestions in terms of using identical questions and procedures in a series of focus group interviews. One suggestion is to use the knowledge gained from completed focus groups to alter and develop both the questions and the route of subsequent focus groups. The other suggestion is to adhere to the same questions and procedures in search of standardisation, which would, as a result, maintain a high level of comparability between the data sets collected (Morgan, 1996, pp.142-143). In this research, focus groups alter and develop both the questions and the route of subsequent

focus groups to gain more perspective on the culture affects on the online privacy perspective and therefore help the designing of the main data collection techniques, i.e. the questionnaire.

4.3.2 RECRUITING PARTICIPANTS

The aim of sampling with respect to focus groups is to ensure the variation of the group's composition. For this reason, focus groups use the strategy of segmentation, which has been inherited from market research, to form groups that consist of particular categories with (mostly) homogeneous characteristics, such as, sex, age, educational level, geographic and / or cultural background. Moreover, segmentation serves as an aid to build a comparative dimension within targeted populations. Segmentation, however, can lead to the creation of a large number of groups, which is time and resource consuming at the level of both data collection and analysis (Morgan, 1996, pp.143-144).

The typical group size of focus groups is between six and ten participants. Moreover, the size of the group depends on the nature of the research. For example, if the research topic is a more emotional subject and consequently requires a higher level of involvement a small number of participants in each group would be preferable. This would give group members more time to discuss their views within an environment that is easy to control. On the other hand if the research topic is more neutral and does not require a high level of involvement it would be better to increase the number of participants in the focus group, which would allow the collection of a wider range of views on the targeted topic (Morgan, 1996, p.146).

With regard to the number of focus groups, it depends on the level of diversity of the targeted participants and topics investigated. In other words, the minimum number of focus groups would increase if participants were needed to represent a wide range of age groups, educational levels, geographic areas or cultural backgrounds or if the investigated topics included different areas that could not be covered in one meeting (Morgan, 1996, pp.143-144).

A set of three focus groups were established to provide a basis for developing survey questions as well as to enrich the literature review by adding open considerations of the cultural and social features that affect the individual's privacy perspective with regard to internet usage (Hill et al.,1998, pp.29-38).

Each focus group consisted of four to six participants who represent Muslim religion from Arabic social background. All groups used Arab-Muslim participants. Unfortunately there was no participants from Malaysia, however one from the participants is Arabic and live in Malaysia and married Malaysian wife. In order to invite and select participants, e-mails were sent to targeted students at both De Montfort and Leicester Universities asking volunteers to participate in focus groups. A group of English language students were contacted and invited to join the second and third focus groups. Participants for the focus groups were selected as a sample of the target participants for the study's main data collection method, the questionnaire (Zakaria *et al*., 2003, pp.66-67). The formal invitation included information about the aim of the research as well as details of the goals and structure of the focus groups (sees Appendix A).

In these focus groups, the number of participants per group was 4-6 (including males and females) university students, members of staff and employees. They were invited by either e-mail or personal invitation. Table 4.1 summaries the gender, nationality, education level and marital status of the focus groups' participants.

Table 4-1: Summary of participants' characteristics

Name	Sex	Education	Marital Status
A	Male	PhD	Married
B	Male	PhD	Single
C	Male	Undergraduate	Married
D	Male	Masters	Married
E	Female	Masters	Single
F	Male	Masters	Married
G	Female	Masters	Single
H	Male	PhD	Married
I	Male	Masters	Single

4.3.3 RECRUITING MODERATORS

The conduct of the moderator or interviewer as well as that of focus group members in their roles with regard to the amount and quality of the data produced places limits on the potential output data of focus groups. For example, unbalanced moderator involvement (either more or less than the optimum) could disrupt the interaction between focus group members. Similarly, an unbalanced involvement of participants

would lead to the exclusion of potential input from hesitant group members. Therefore, there is a need for the moderator to be sufficiently trained to manage a focus group. The focus group itself must be well planned and rehearsed to avoid any potential disruption to the participants' communications (Morgan, 1996, p.140). The researcher moderated the groups.

4.3.4 ANALYSIS AND REPORTING

The proceeding of all three focus groups was recorded and the discussions were transcribed. Phrases and quotations from the transcriptions were juxtaposed with targeted concepts on privacy perspectives. Finally, a discussion of the main factors that might affect an individual's perspective toward privacy was reported.

4.4 OUTCOME

Focus groups can very quickly produce a large amount of recorded data, which is difficult and time consuming to transcribe and analyse (Bryman, 2010, pp.352-358). The difficulty in identifying individual speakers and distinguishing between their arguments is probably one of the most important and specific limitations associated with this methodology (Flick, 2005, p.122).

In table 4.2, we find brief examples of questions and answers from the focus groups regarding the concept of privacy and suggestions of factors that could affect individuals' privacy perspectives.

Table 4-2: Examples of questions and answers from the focus groups

Question 1: Which of the following personal information matters when you try to protect your right to privacy: your name, home address, phone number, mobile phone number, e-mail address, income, religious views and political views?	
Concepts and factors	Phrase or Quote from Answers
	"A: I would not give any religious or political view. B: But sometimes when you fill in a form, they ask about your religion. A: I think it's a way of discrimination, why do they ask about ethnic origin and religion, it is discrimination." "A: In the UK (not in my country), home address, e-mail address, phone number (and) no problem with my religion ..." "I have added as a moderator that: some websites ask about your income." C: ... "I will be just closing the browser, it is not necessary...." "D: ... In my opinion I do not mind giving any personal information but that could increase the SPAM..." "E: ... I have never been in a situation where I have to give my mobile number (when I search for information using the Internet)." "F... For me I think it depends who wants the information... and its history of giving me benefits."
Question 2: Have you experienced a situation where you felt that your privacy or the privacy of somebody you know has been violated in some way? If yes, could you briefly explain what happened and why you felt it violated the right to privacy?	
Privacy Perceptions	Phrase or Quote from Answers
Economical	"C: I have a personal experience, I have a credit card and someone started charging me for using my card, ...and I found someone have another card .... I found 4 credit cards under my name ..."
Sociological	"G: My friend, actually her password .... somehow, someone knows her e-mail password ... and started sending bad messages to us using her e-mail address."
Psychological	"H: I have, as a sub-warden [at university accommodation], where one of my colleagues talked about a mental problem of a student in the accommodation, I was not happy about that. The student wanted to sue the university, and I had to take it to the university"
Question 3: Ahmad looks at the chat files on his personal computer, which include all the Microsoft Messenger chats that his wife had with her sisters and friends, and he enjoys reading what they say about their husbands, kids and friends, with no intention whatsoever to use, disclose or even mention this very ordinary information to his wife or anyone else. In this case or similar ones, do you think that Ahmad violated his wife's right to privacy?	
Privacy Dimensions	Phrase or Quote from Answers
Intimacy	"H: It is not right and trust must be between wife and husband, but it depends on the trust between them."
Solitude	"E: Sometimes you want to keep your privacy to yourself."

Reserve	"G: A secret is a secret, [if she wants him] to know she will tell him…)
Reserve	"C: It hurts physically ... [...]... and even emotionally, for example I sometimes complained about my father and mother, but I do not want them to hear what I said, and also for wife and husband..."

Question 4:

Samer worries about recent changes in his teenage son's behaviour as he spends all his time either online or outside the home. After many failed attempts to understand what is wrong with his son, for example by asking him and by talking to his companions, Samer has decided to ask his friend, who is a computer technician, to help him to break into his son's laptop. Do you think that Samer has the right to breach his son's right to privacy? Why?

Privacy Dimensions	Phrase or Quote from Answers
Solitude	"A: I agree with him and he has the right to protect his teenage son."
Solitude	"C: ... He wants to protect him and watch him before getting involved in bad situation..."
Intimacy	"A: It is related to our culture and religion, the father has the right to [know] about his son..."
Intimacy	"D: ...But what if the son finds out, he will be more angry and will cause more problems ... and he will not trust you again..."
Reserve	"F: ...If you feel that you are losing your son and you feel that he's going in the wrong direction, you would not say I am not going to break my son or daughter's privacy. Of course you would care about breaking it, you would do everything just to make sure... he's not your friend (or somebody else's) that if he's fine it is fine, if I lose him I do not care, he's your son.... [interrupting]: it is your responsibility…"

Question 5:

Abdullah studies at a college outside of his city. He enjoys communicating with his family back home using Microsoft Messenger. One day he added a web camera to his PC in order to be able to see his family members but his sister Eman refused to appear on the camera.

Do you think that this is a common practice within your family and friends? Why?

Privacy Dimensions	Phrase or Quote from Answers
Seclusion	"F: For me, as a Muslim, my sister... maybe sometime worries about using the camera because there is a hacker who could get the picture and use it in a bad way."
Reserve/ Anonymity	"I: ... She might walk in the street without covering her face, but it's a kind of privacy that we were talking about, it is like your e-mail, nothing wrong about it, but you do not want anybody to see it..."

Question 6:

In a place like prison, the prisoners are observed all the time by the guards, who, at the same time, restrict others from any informational and physical access to these prisoners. Do you think that we could claim that these prisoners have privacy? Why?

Nothing has been quoted for this question, as all answers were irrelevant. The participants discussed

whether the prisoners had the right to privacy or not, whereas the aim of this question was to examine whether the participants were aware of the concept of privacy.	
Question 7:	
Do you think privacy can be maintained? What do you think can maintain the right to privacy: the law and regulation, religious background or the development of information technology?	
Privacy Factors	Phrase or Quote from Answers
Religious motivation	"C: ... If you are Muslim and we have our privacy, then the law is only out for the public, and then the technical development." "I: ... Religion, because it starts from the person himself, and secondly technical…"
Technical knowledge	"D: The first thing is the technical development, because we cannot control the law..."

4.5 DISCUSSION

The main aim of the research investigation was to discover whether the relationship between privacy and ICT is affected by the individual's cultural contexts. In this initial investigation, the cultural influences that affect the privacy perspectives of individuals upon their internet usage were studied together with the similarities and differences in these perspectives towards the issue of privacy within ICT usage between people of different cultural backgrounds. The outcome of the focus group analysis can be divided into two main sets of concepts: first, individual online privacy perspectives and second, the impact of culture in shaping individuals' online privacy perspectives.

With regard to individuals' online privacy perspectives, although the participants agreed upon what is considered personal information they were divided on what they would be prepared to reveal. Some of them would not reveal sensitive data, such as, religious or political points of view and others would not disclose, in some situations, their personal data, such as, home address and telephone number. In addition, participants' attitudes with regard to submitting personal information that was mandatory were varied. For example, when the participants were asked what would they do if the website required

them to provide their name, home address, phone number, mobile phone number or e-mail address. In response to this question D said, " ... In my opinion I do not mind giving any personal information ..." whereas M said, " ... I will be just closing the browser..." and A said, " in the UK (not in my country), home address, e-mail address, phone number [and] no problem with my religion ...".

With respect to the perspectives that form the importance of privacy among the participants, three perceptions have been identified. The economical perspective, "I have a credit card and someone started charging me for using my card …and I found someone have another card ...." The sociological perspective, "...somehow, someone knows her e-mail password ... and started sending bad messages to us using her e-mail address." The psychological perspective, "... one of my colleagues talked about a mental problem of a student in the accommodation, I was not happy about that. The student wanted to sue the university, and I had to take it to the university.".

In addition, such attitudes as whether or not to provide personal information to a website seems to depend on the individual's level of the privacy concerns and Internet trust toward the website. For example, F said "... but that could increase the SPAM..." and F said "... for me I think it depends who wants the information... and its history of giving me benefits." In line with these statements, Smith et al., (1996, p.189) claim that this type of personal information could affect an individual's privacy concerns and Internet trust levels whereas Dinev and Hart (2003, p.6) and Siala et al., (2004, pp.8-9) studied the effect of the level privacy concerns and Internet trust on the level of Internet activities.

Questions three, four and five reveal four of the six dimensions for measuring of privacy. They are illustrated by the following examples.

The first of these privacy dimensions is the freedom from others' surveillance (intimacy) and is illustrated by the following two examples. First, one participant's answer to question three, namely, whether it is right or not to read a wife's online chat files was, "It is not right and trust must be between wife and husband but it depends on the trust between them." Second, other participants' answered question four, that is, whether it is right or not to hack the son's computer in order to protect him. One participant said, "...the father has the right to [know] about his son."

The second and third privacy dimensions are the level of freedom from others' surveillance (solitude) and the ability to limit disclosure to others (reserve). In particular, one of the participant's answers to questions four was, "...but what if the son finds out, he will be angrier and will cause more problems ... and he will not trust you again..."

The fourth privacy dimension is the visual and auditory privacy of the home (seclusion) and was illustrated in particular by one participant's answer to question four, about the female refusal to use a web camera. He said "...for me as a Muslim, my sister... maybe sometime worries about using the camera because there is a hacker who could get the picture and use it in a bad way"

Furthermore, the focus group participants identified a number of forms of possible violations of their privacy by unauthorised and improper use of their personal information (Dinev and Hart, 2006, p.7) that included fraud, hacking and unethical usages of personal information. For example, when asked if they had experienced a situation, where they felt that their privacy or the privacy of somebody they knew has been violated in some way, one of them mentioned a personal experience of credit card fraud. Another participant pointed out that her friend had her e-mail hacked and another participant told the story of someone who leaked sensitive information about a psychological problem of a student in the accommodation where he resides.

Regarding the possible effect of culture on individuals' online privacy perspectives, participants varied in their views of what the effect of maintaining and preventing privacy could be. For example, C said, "...if you are Muslim and we have our privacy, then the law is only out for the public, and then the technical development." I said, "... religion, because it starts from the person himself and secondly technical." D said, "... the first thing is the technical development, because we cannot control the law..." The effect of religious beliefs, Internet regulation and IT skills on privacy concerns and Internet trust have been studied by a number of researchers (Milberg et al., 2000; Chan *et al.*, 2002; Zakaria *et al.*, 2003; Bellman et al., 2004; Wirtz *et al.*, 2007; Dinev and Hart, 2006; Al-A'ali, 2008).

In summary, from the initial finding of the focus groups and the literature review, the privacy perspective seems to consist of the concept of what is personal information, online privacy concerns and online trust, which seem affected by Internet users'

families and friends (social norms), religious beliefs, IT skills and the nature of their local Internet regulation and demographic factors (Figure 4.1).These factors are the main cultural affect on the online privacy perspective that would be studied in this research. Later, in the following chapter, these factors would be used in the designing of the main research instrument in this study, i.e. questionnaire.

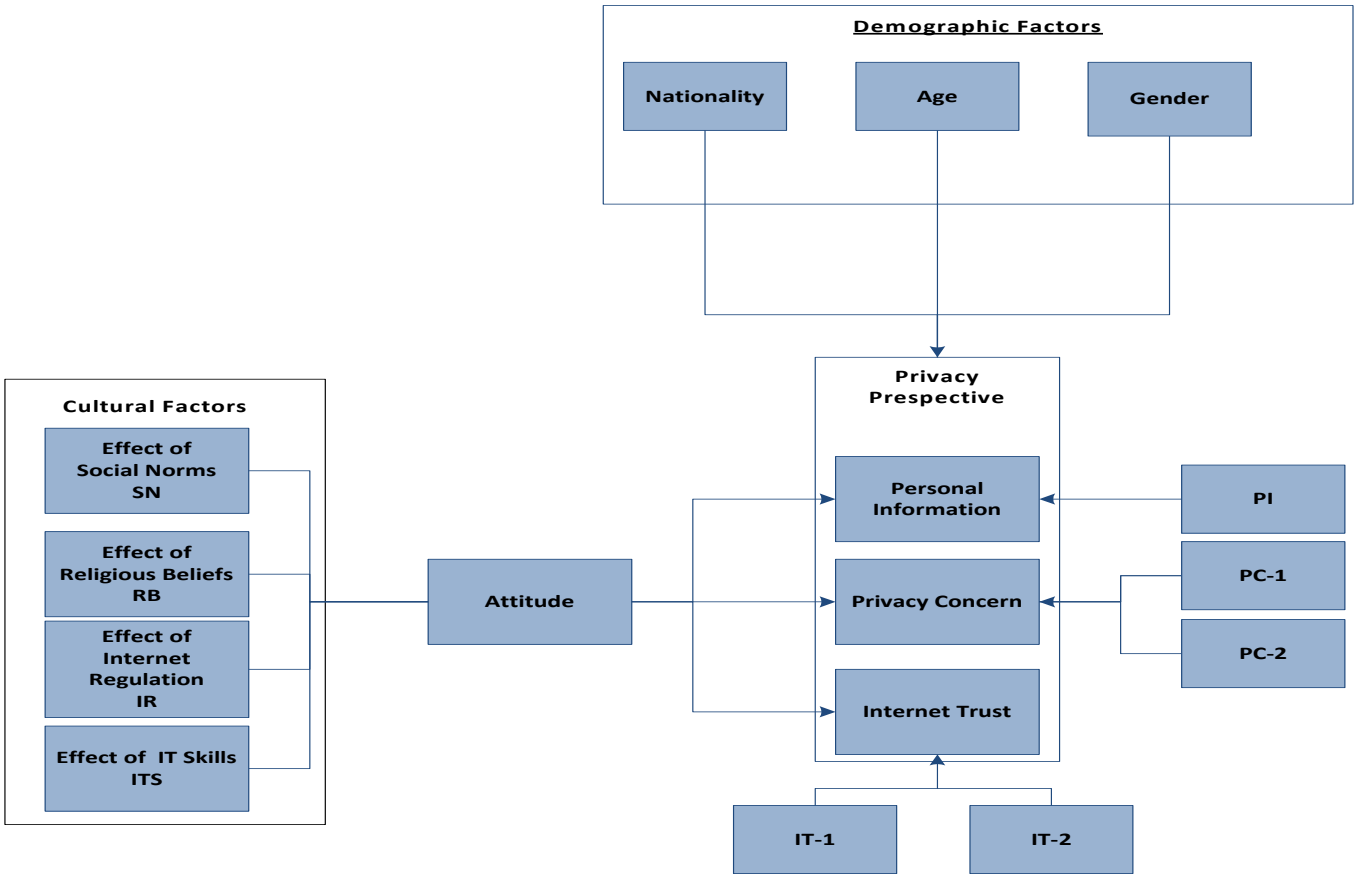


Figure 4-1: The Effect of Cultural Back ground and Demographic Factors on the Online Privacy Perspective

4.6 CONCLUSION

In this chapter the use of the focus group method as a preparation for the primary method of this research, that is, the questionnaire survey, was illustrated. This included, first, a brief comparison between focus groups, surveys and individual interviews. This was followed by a discussion on the use of focus groups as a social research strategy for this study's research question and planning strategy. The issues to be considered included those associated with using focus groups as a social research method, such as, standardisation, sampling, group size and number of groups. Finally, the chapter closed by giving an outline and analysis of the main outcomes of the focus groups.

Focus group discussions show that the online privacy perspective consists of three elements: personal information, online privacy concerns and the trust. These discussions also showed that a number of factors affected their privacy perspectives. These factors include the cultural background of Internet users, which includes social norms, religious beliefs, IT skills and their local Internet regulation. In chapter five, these outcomes employed alongside the literature review will be used to identify the research variables, model and hypothesis for studying the relationship between the individual's online privacy perspective and the cultural affect on their online privacy attitudes.

5 CHAPTER 5: RESEARCH DESIGN

5.1 INTRODUCTION

Chapter two underlined a number of topics in relation to the research aims, which are the investigation of the relationship between privacy and the Internet and the effect upon it of the cultural backgrounds of individuals in Islamic cultures (1.3 Research Motivation and Aims). First, chapter two highlighted a number of relationships between privacy, ICT and culture. Then, the concept of online privacy perspective including the role of the nature of online personal information, the online information-provider and collector were discussed. Finally, in chapter two, a profile of Saudi Arabia and Malaysia was provided, being the countries from which the target participants were drawn.

Chapter three discussed the research methodology, including its philosophical paradigms and quantitative and qualitative research strategies, including some of their associated research methods and data collection techniques, such as, the interview, questionnaire, case study and focus group. Chapter 3 concluded by selecting the positivist paradigm, a quantitative methodology using the survey method and the questionnaire as the data collection strategies and analytical techniques for this research.

In chapter four, the initial data collection and the focus group's outcomes were discussed. This consisted of the online privacy perspectives: personal information, online privacy concerns and online trust. In addition, the effect of the cultural background of the Internet users, which includes social norms, religious beliefs, IT skills and their local Internet regulation.

Based on the discussion in chapters two, three and four this chapter aims to discuss some important issues relating to the design of the survey, that is, the research aim, questions, variables and hypotheses. This chapter will cover the design and validation of the questionnaire instrument, its translation and the data collection process.

5.2 RESEARCH AIMS AND QUESTIONS

As was mentioned in the introductory chapter, the purpose of this study is to investigate the relationship between online privacy perspectives and how they are affected by the cultural surroundings of the individual. It has been designed to: (1) identify cultural influences that affect the privacy perspectives of individual Muslims in their use of the Internet; (2) identify similarities and differences between the perspectives of individual Muslims with different cultural backgrounds, namely, Saudi and Malaysian cultures towards the issue of privacy within Internet usage.

For this purpose, four research questions were formulated. The first question is: Is there a relationship between the level of an individual's concern over Internet privacy and the effects of their religious beliefs, IT skills, the social norms and the local Internet regulation that affects their attitudes to online privacy? The second question is: Is there a relationship between the level of an individual's trust of the Internet and the effects of their religious beliefs, IT skills, the social norms and the local Internet regulation that affects their attitudes to online privacy? The third question is: how do religious beliefs, IT skills, social norms and Internet regulation affect their Internet privacy concerns and Internet trust? The fourth question is: in this research what are the similarities and differences between individual Muslims from different cultural backgrounds with

regard to the effects of their religious beliefs, IT skills, the social norms and local Internet regulation on both their Internet privacy concerns and their Internet trust?

Given that the research aim is to, "Investigate the relationship between online privacy perspectives and the Internet and how these are affected by the individuals' cultural surroundings" and given that the selected research methodology is a quantitative one, the research investigation was, therefore, done by measuring "the online privacy perspective" as a number of dependent variables, "the effect of cultural background on the online privacy attitude" as a number of independent variables and "the age, gender and nationality" as demographic variables as mentioned in the previous chapter (section 4.5) and described in Figure 4-1 (see also Figure 5.1, for a convenient repetition). This model would be tested on participants from Saudi Arabia and Malaysia (See section 5.7) using a self-completion questionnaire (see section 5.6). This was achieved via a questionnaire in order to measure the relationship between them. In the next section, the research variables and model are illustrated.

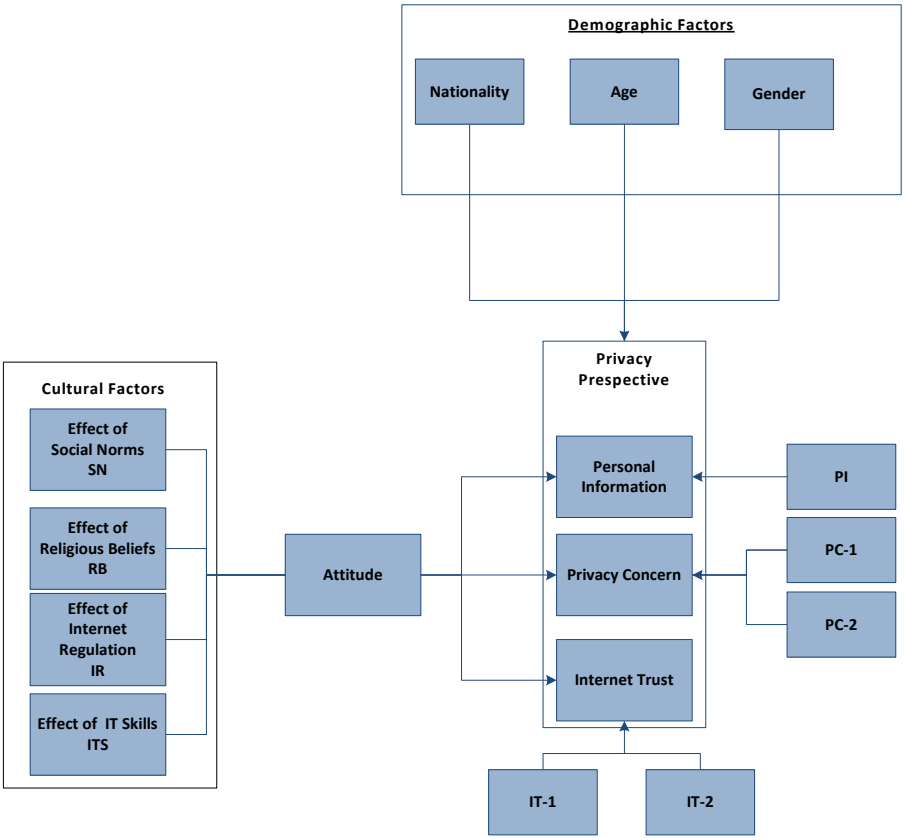


Figure 5-1: The Effect of Cultural Back ground and Demographic Factors on the Online Privacy Perspective

5.3 RESEARCH VARIABLES AND HYPOTHESES

The literature review shows that the online privacy perspective could be formed as the calculus of the privacy concern, Internet trust and the type of personal information (Smith *et al.*, 1996, p.189 and Dinev and Hart, 2006, pp.63-64). According to the outcomes of the focus groups, the type of the personal information could affect the level of both privacy concern and Internet trust. For example, as mentioned in Chapter four (section 4.5) and in the answer to whether or not to submit personal information to a website, a participant said, *"... but that could increase the SPAM..."* and another said, *"... for me I think it depends who wants the information... and its history of giving me*

benefits." The online privacy perspective, therefore, is formed by three perceptions, which are personal information online, privacy concerns and Internet trust (Figure 5.2).

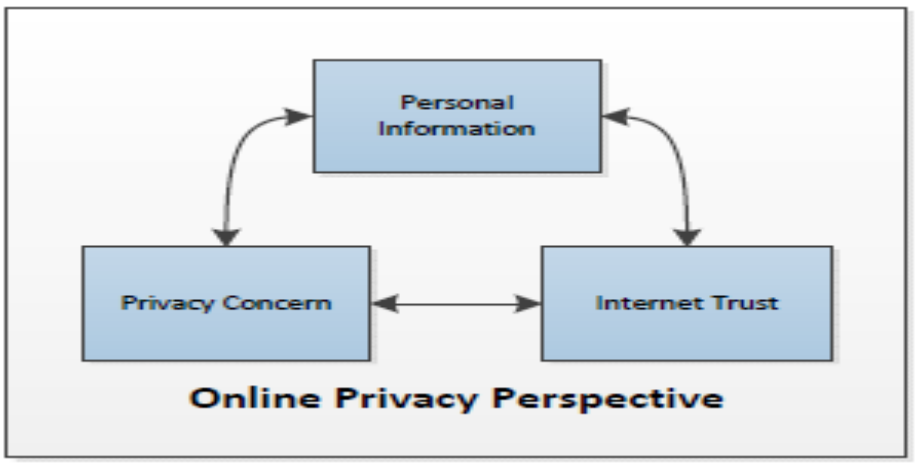


Figure 5-2: The Three Perceptions of the Online Privacy Perspective

According to Dinev and Hart (2006), and Xu *et al.* (2008), both privacy concern and Internet trust are measured by two factors (Table 5.1). Privacy concern is measured by Internet users, concerns about submitting personal information online and their concerns about the possible unexpected, unauthorised or improper secondary use of the submitted personal information. Internet trust is measured by Internet users' concerns regarding the disclosure of personal information online and Internet users' trust regarding the safety of the exchange of information with others online (Dinev and Hart, 2006 and Xu *et al.*, 2008).

Table 5-1: The Three Perceptions That Form Online Privacy Perspective

Perceptions	Factors/ Measurements	References
Personal Information	Personal information	Smith *et al.*, (1996) and Dinev and Hart, (2003)
Privacy Concerns	Internet users' concerns about submitting personal information online	Dinev and Hart (2006), and Xu *et al.* (2008)
	Internet users' concerns about the possible unexpected, unauthorised or improper secondary use of the submitted personal information	
Internet Trust	Internet users' concerns about handling personal information online	
	Internet users' trust of the safety of the exchange	

Therefore, five dependent variables are formed as the online privacy perspective's variables. They are the personal information **(PI)**, the Internet user's concerns about submitting personal information online **(PC-1)**, their concerns about the possible unexpected, unauthorised or improper secondary use of the submitted personal information **(PC-2)**, Internet user's concerns about handling personal information online **(IT-1)** and the Internet user's trust about the safety of the exchange **(IT-2)** (Figure 5.3).

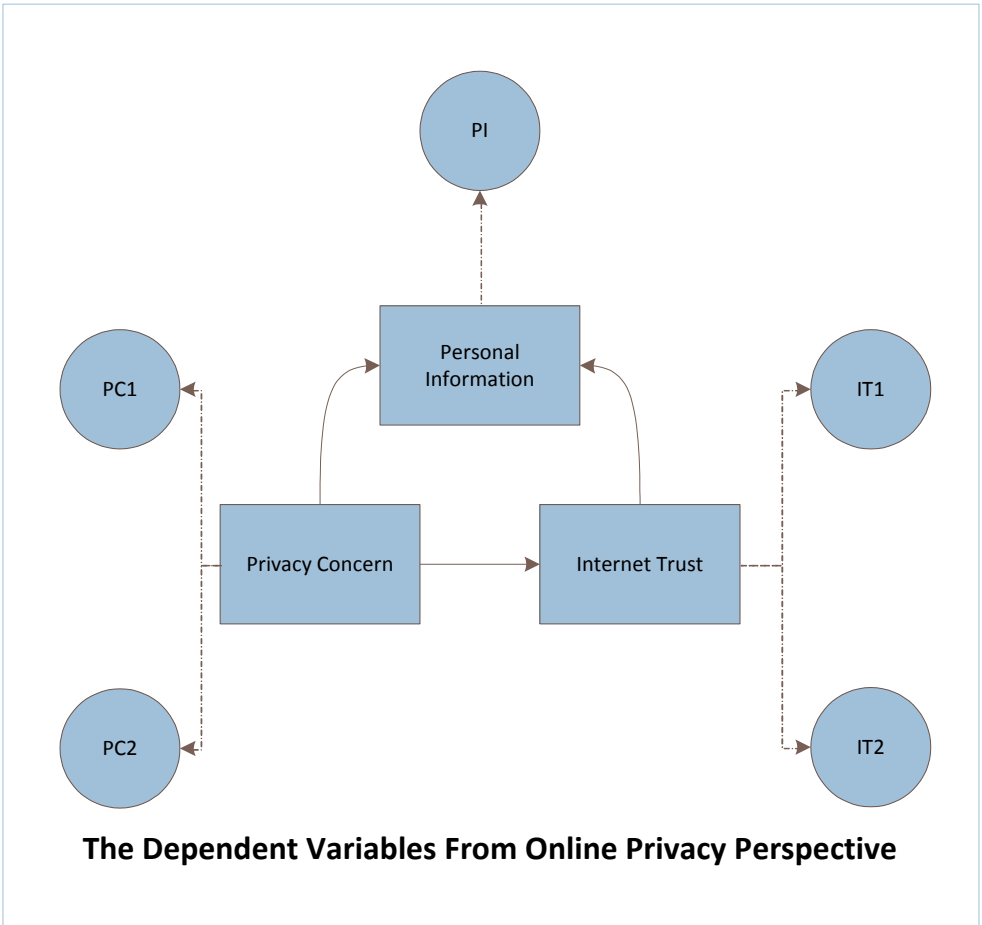


Figure 5-3: The Five Dependent Variables for the Online Privacy Perspective

Furthermore, the literature review confirms that the adoption of ICT, utilising the Internet and the perspective of online privacy are influenced by cultural backgrounds (Milberg *et al.*, 2000,, Zakaria *et al.* 2003, Ballman *et al.*, 2004, Hubona *et al.*, 2006, Loch, *et all*, 2003, Dinev *et al.*, 2005, Siala *et al.*, 2004 Wirtz *et al.*, 2006). As mentioned in section (2.3.2), cultural background could include a number of elements, such as facts, symbols, norms and values in a particular society (Hofstede, 1984, p.18 Zakaria *et al.* 2003, p.52) it, also, could consists of four compounds: social norms, religious beliefs, IT skills and the perception of Internet regulation based on the

following definition of culture, *"The quintessence of the physical resources and perceptions of the physical and mental techniques, which allow a society to persist."* (Stahl and Elbeltagi, 2004, p.48). Give that the above mentioned Stahl and Elbeltagi, (2004, p.48) definition of cultural background, provides a measurable elements of culture, i.e. religious belief, social norms, regulation both by government and by corporations (Ehereneich, 2001) see section (2.3.4) and skills, this definition of cultural back ground is applied in this research.

The outcomes of the focus groups show support for the perception of the effect of social norms, religious beliefs, IT skills and Internet regulation on privacy, that comes from the above mentioned Stahl and Elbeltagi, (2004, p.48) definition of cultural background, for example, a participant from the focus group (mentioned in section 4.4) insisted that *"... if you are Muslim and we have our privacy, then the law is only out for the public, and then the technical development"*, another said*,"... religion* [is the main factor], *because it starts from the person himself and secondly technical.",* and another participant argued that*"... the first thing is the technical development, because we cannot control the law..."*. Therefore, the effect of social norms, religious beliefs, IT skills and the perception of Internet regulation on online privacy are the other four independent variables in the investigation of this research (Figure 5.4).

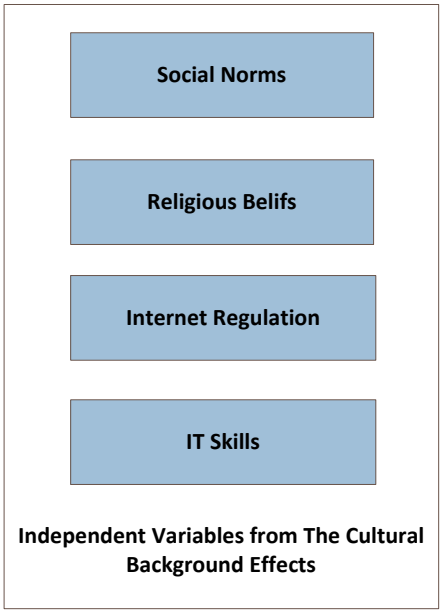


Figure 5-4: The Four Independent Variables for the Cultural Effects

These independent variables are studied by measuring the effect of social norms, religious beliefs, Internet regulation and IT skills on online privacy attitudes (Table 5.2). The social norm effect is defined as the effect of family and friends on online privacy attitudes. The religious belief effect is defined as the effect of Islamic law (Sharia), according to the participants' points of view, towards their online privacy attitudes. The Internet regulation effect is defined as the effect of Internet regulation in the participants' own countries on their online privacy attitudes. The IT skills effect is defined as the effect of participants' IT skills on their online privacy attitudes.

Table 5-2: Independent Variables

Independent Variables	Factors	References
Social norms	The effect of social norms on online privacy attitudes	Ballman *et al.*, 2004, Dinev *et al.*, 2005, Siala *et al.*, 2004, and Xe *et al.*, 2008
Religious beliefs	The effect of religion on online privacy attitudes	
IT skills	The effect of IT skills on online privacy attitudes	Ballman *et al.*, 2004 and Dinev and Hart, 2006
Internet regulation	The effect of the perception of Internet regulations on online privacy attitudes	Milberg *et al.*, 2000, and Wirtz *et al.*, 2006, pp. 340-341

In this study, online privacy attitudes are defined as an individual's intentions and acts to keep personal information private online, care about one's online privacy and others' online privacy and being careful when revealing personal information (Xe *et al.*, 2008). Therefore, each of the independent variables, which are the effects of social norms, religious beliefs, Internet regulation and IT skills on online privacy attitudes would be measured with regards to their effect on attitudes; keeping personal information (KPI), caring about their privacy online (CATPO), caring about others' online privacy (CAOPO) and being careful when revealing personal information (CWRPI) (Figure 5.5).

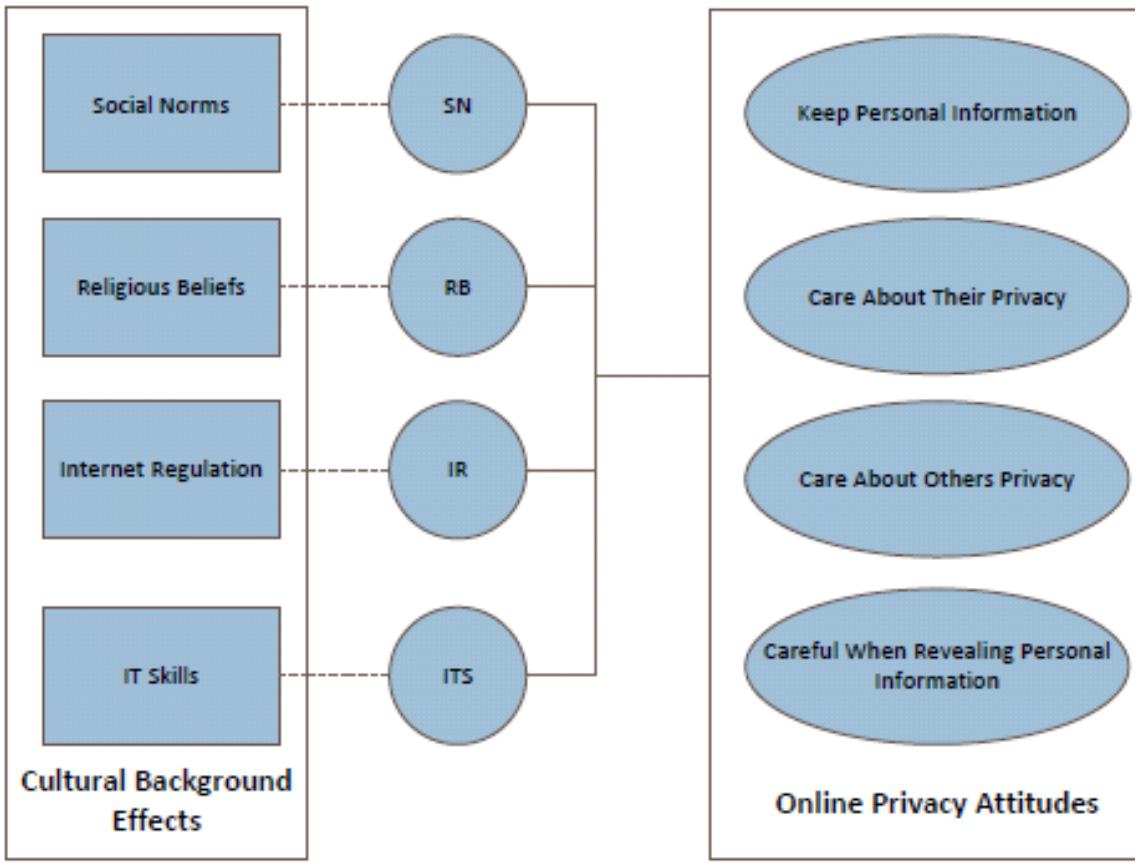


Figure 5-5: Independent Variables from The Cultural Background Effects on The Online Privacy Attitudes

Furthermore, age, gender and Internet experience tend to affect the level of online privacy (Newell, 1998, p.366; Bellman, 2004, pp.313-324 Stahl, 2008, pp.51-52). Therefore, they will be demographic variables.

In summary, this research investigates the relationship between five main dependent variables that form the online privacy perspective together with four independent variables that represent the cultural effects of online privacy attitudes and three demographic factor/ variables (Figure 5.6).

The dependent variables in this research are:

1) The Internet user's perception with regard to what is personal information (PI)

2) The Internet user's concerns over submitting personal information online (PC1)

3) The internet user's concerns over the possible unexpected, unauthorised or improper secondary use of any submitted personal information (PC2)

4) The Internet user's concerns over handling personal information online (IT1)

5) The Internet users concerns over the safety of the exchange of information with others online (IT2)

The independent variables in this research are:

1) The effect of social norms (SN)

2) The effect of religious beliefs (RB)

3) The effect of Internet regulation (IR)

4) The effect of IT skills on online privacy attitudes (ITS).

The demographic factors are age, gender and nationality.

The final research model is illustrated in figure 5.6. It shows that the five components of the online privacy perspective (IP, PC-1, PC-2, IT-1 and IT-2) of the Internet users are affected by the impact of the four cultural background components (SN, RB, IR and ITS) on the four online privacy attitudes (KPI, CATPO, CAOPO and CWRPI) and the demographic characteristics (age, gender and nationality) of the Internet users.

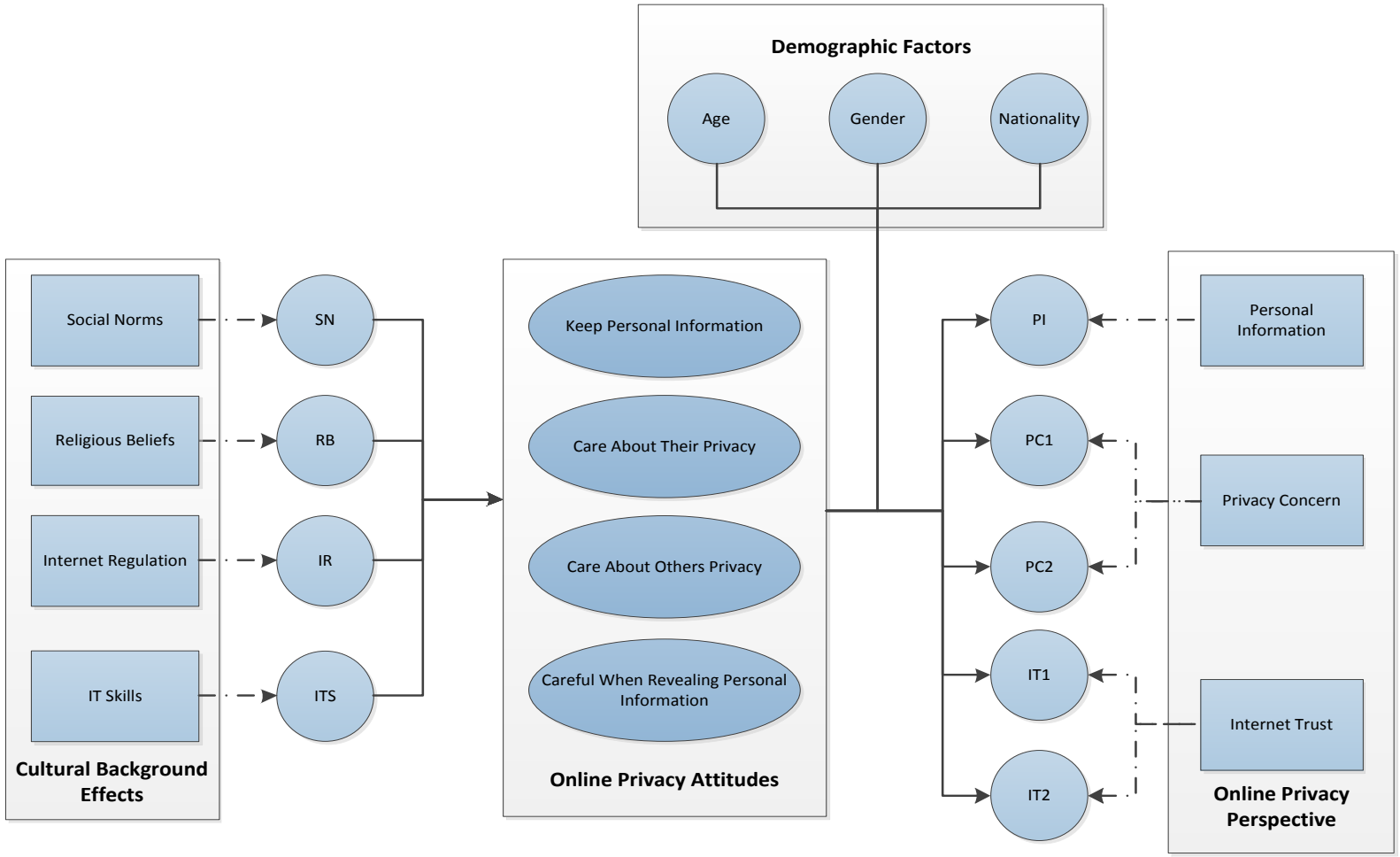


Figure 5-6: Dependent, Independent and Demographic Variables

In summary, this research proposes five dependent variables, IP, PC1, PC2, IT1 and IT2, four independent variables SN, RB, IR and ITS, and three demographic variables, Nationality, gender and age. In the next section, the research hypotheses will be discussed and related to the research model.

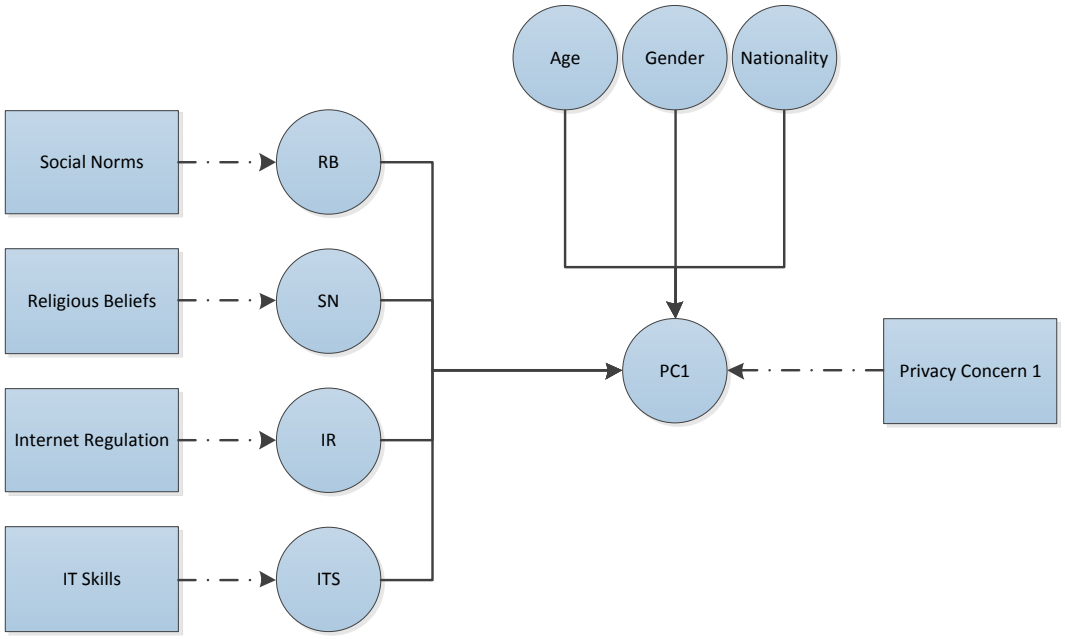
5.4 RESEARCH HYPOTHESES

As mentioned at the beginning of this chapter, the purpose of this study is to investigate the relationship between privacy and the Internet and how individuals' cultural backgrounds affect it. To explore these issues, the following hypotheses are proposed under each of the research questions mentioned in section (1.4 Research Questions).

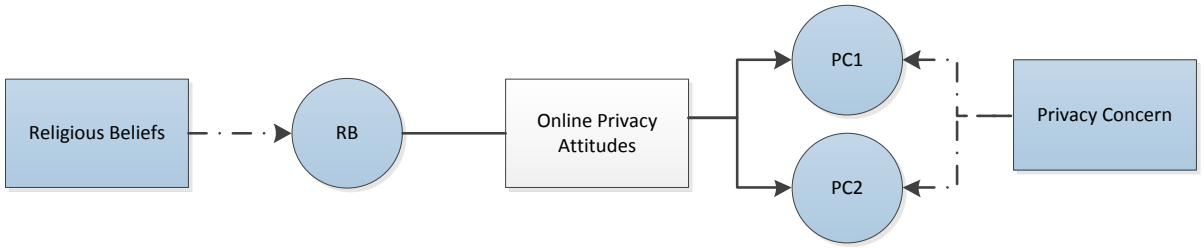
The hypothesis could be one-tailed, two-tailed or null hypothesis. Basically, using one-tailed hypothesis is better than the two-tailed and null hypothesis in the power of prediction. For example one tailed needs to use the $p<0.05$ to have the same statistical power of the two-tailed/ null hypothesis of $p<0.025$, as with the latter, the probability is split into two directions. However this power of the one-tailed hypothesis is only beneficial if the right direction is selected. This could be because the other direction does not make sense or cannot be investigated (Leventhal, Huynh, 1996, pp. 278-292, Field, 2009, pp. 28-29, Lombardi, and Hurlbert, 2009, pp. 447, and Gravetter and Wallnau, 2009, p.257,). Giving that this research is interested in investigating the possibility of the increase in the privacy concerns (PC-1 and PC-2) and in the Internet trust (IT-1 and IT-2) due to the increase in the cultural affects social norms (SN), religion beliefs (RB), Internet regulation (IR) and IT skills (ITS), not the other way around, hypotheses in this research, are consider as a directional (one-tailed) hypotheses.

5.4.1 HYPOTHESES FROM RESEARCH QUESTION ONE

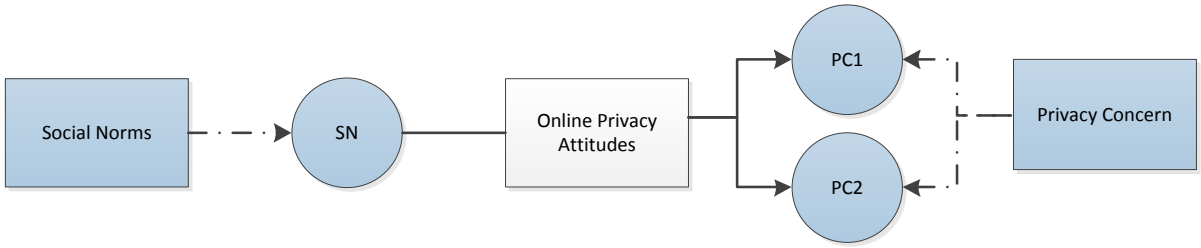
Research Question 1: Is there a relationship between the level of an individual's Internet privacy concerns and the effects of their religious beliefs, IT skills, social norms and local Internet regulation on their online privacy attitudes?



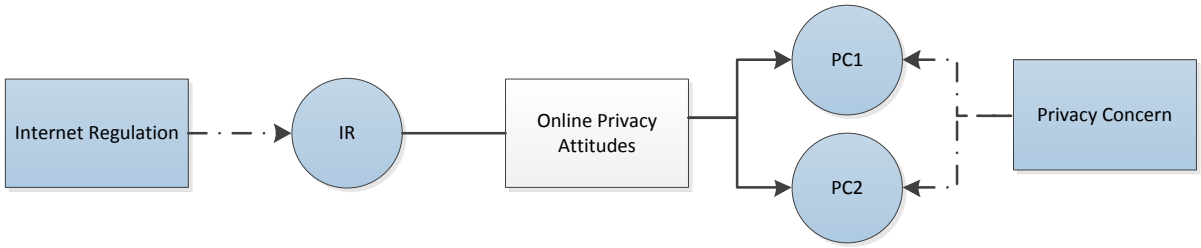
H1: A higher level of Internet privacy concern is related to the greater impact of an individual's religious beliefs on their online privacy attitudes.



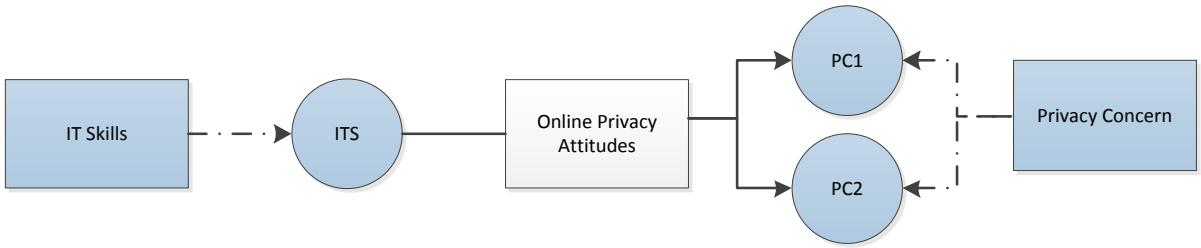
H2: A higher level of Internet privacy concern is related to the greater impact of social norms on an individual's online privacy attitudes.



H3: A higher level of Internet privacy concern is related to the greater impact of local Internet regulation on an individual's online privacy attitudes.

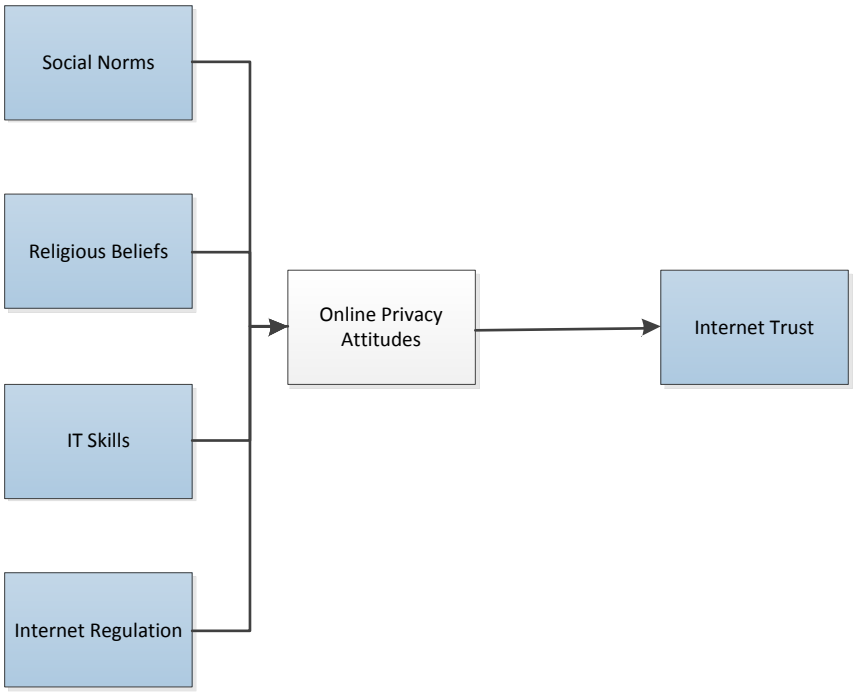


H4: A higher level of Internet privacy concern is related to the greater impact of an individual's IT skills on their online privacy attitudes.

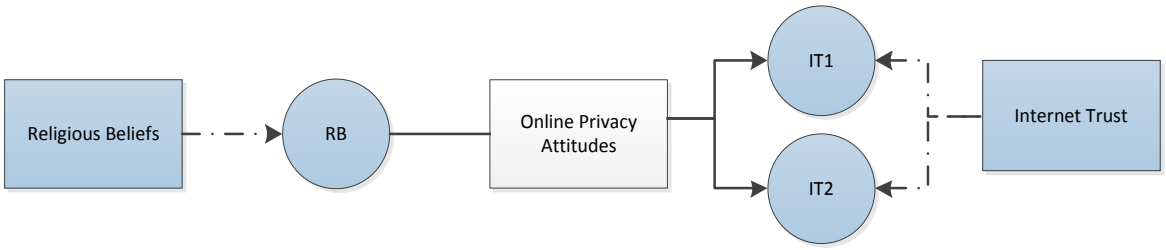


5.4.2 HYPOTHESES FROM RESEARCH QUESTION TWO

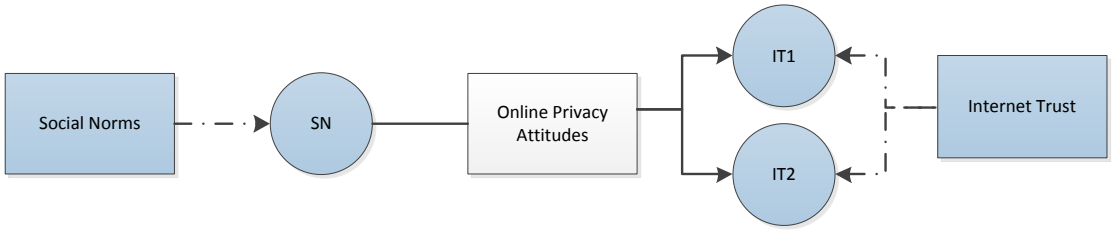
Research Question 2: Is there a relationship between the level of an individual's Internet trust and the effects of their religious beliefs, IT skills, social norms and local Internet regulation on their online privacy attitudes?



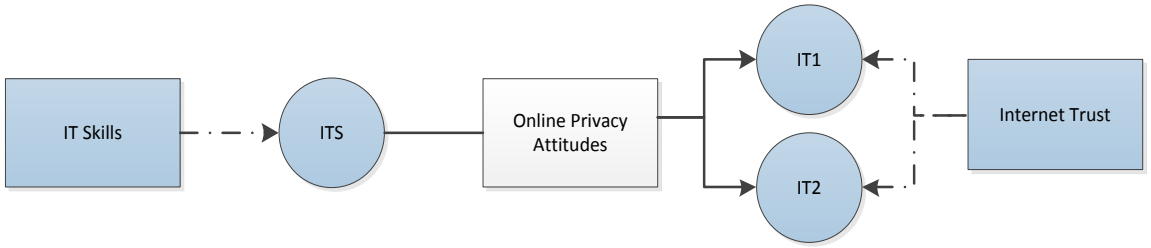
H5: A higher level of Internet trust is related to the greater impact of an individual's religious beliefs on their online privacy attitudes.



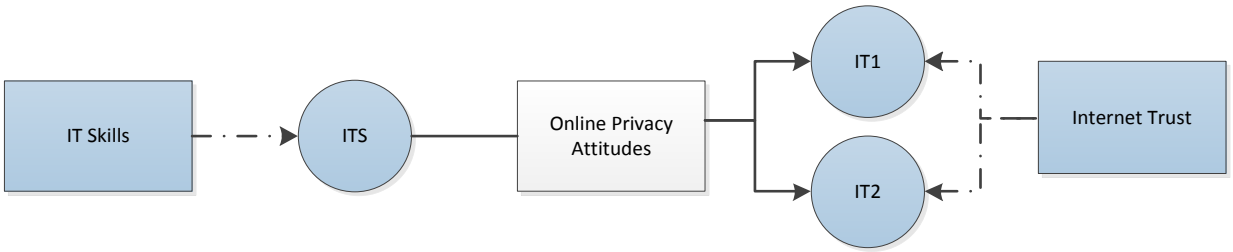
H6: A higher level of Internet trust is related to the greater impact of social norms on an individual's online privacy attitudes.



H7: A higher level of Internet trust is related to the greater impact of Internet regulation on an individual's online privacy attitudes.



H8: A higher level of Internet trust is related to the greater impact of an individual's IT skills on their online privacy attitudes.



5.4.3 HYPOTHESES FROM RESEARCH QUESTION THREE

Research Question 3: To what extent do an individual's religious beliefs, IT skills, social norms, local Internet regulation and their impact on the individual predict their Internet privacy concerns and their Internet Trust?

H9: The effect of the Internet user's religious beliefs on their Internet privacy concerns is greater than that of other factors, that is, IT skills, social norms and Internet regulation.

H10: The effect of the Internet user's social norms on their Internet privacy concerns is greater than that of other factors, that is, IT skills, religious beliefs and Internet regulation.

H11: The effect of the Internet regulation in an Internet user's country on their Internet privacy concerns is greater than that of other factors, that is, the religious beliefs, IT skills and social norms.

H12: The effect of the Internet users' IT skills on their Internet privacy concerns is greater than that of other factors, that is, their religious beliefs, social norms and Internet regulation.

H13: The effect of the Internet users' religious beliefs on their Internet trust is greater than that of other factors, that is, their social norms, Internet regulation and IT skills.

H14: The effect of the social norms on Internet users on their Internet trust is greater than that of other factors, that is, their IT skills, religious beliefs and Internet regulation.

H15: The effect of the Internet regulation in force in an Internet user's country on their Internet trust is greater than that of the other factors, that is, their religious beliefs, IT skills and social norms.

H16: The effect of the Internet users' IT skills on their Internet trust is greater than that of other factors, that is, their religious beliefs, social norms and Internet regulation.

5.4.4 HYPOTHESES FROM RESEARCH QUESTION FOUR

Research Question 4: What are the similarities and differences between individual Muslims, from different cultural backgrounds, with regard to the effects of their religious beliefs, IT skills, social norms and local Internet regulation on both their Internet privacy concerns and their Internet trust?

H17: The influence of the individual's religious beliefs over their privacy perspective is greater for those in Malaysia than for those in Saudi Arabia.

H18: The influence of social norms on the individual's privacy perspective is greater in Malaysia than in Saudi Arabia.

H19: The influence of Internet regulations over the individual's privacy perspective is greater in Malaysia than in Saudi Arabia.

H20: The influence of the individual's IT skills over their privacy perspective is greater in Malaysia than in Saudi Arabia.

5.5 THE RESEARCH MODEL

According to the above variables and hypotheses, the suggested research model includes the following points (Figure 5.7):

1. The privacy perspective consists of two aspects. These are privacy concerns and Internet trust.
2. Privacy concerns consist of what is considered personal information (P1), with regard to submitting it via the Internet (PC) and about its unauthorised use (PC-2).
3. Internet trust consists of trust with regard to the professional handling of personal information (IT) and in the safety of its exchange via the Internet (IT-2).
4. Cultural factors that might affect online privacy attitudes and, therefore, the privacy perspective are religious beliefs (RB), social norms (SN), Internet regulations (IR) and IT skills (ITS).
5. Demographic factors that might affect online privacy attitudes are nationality, age and gender.

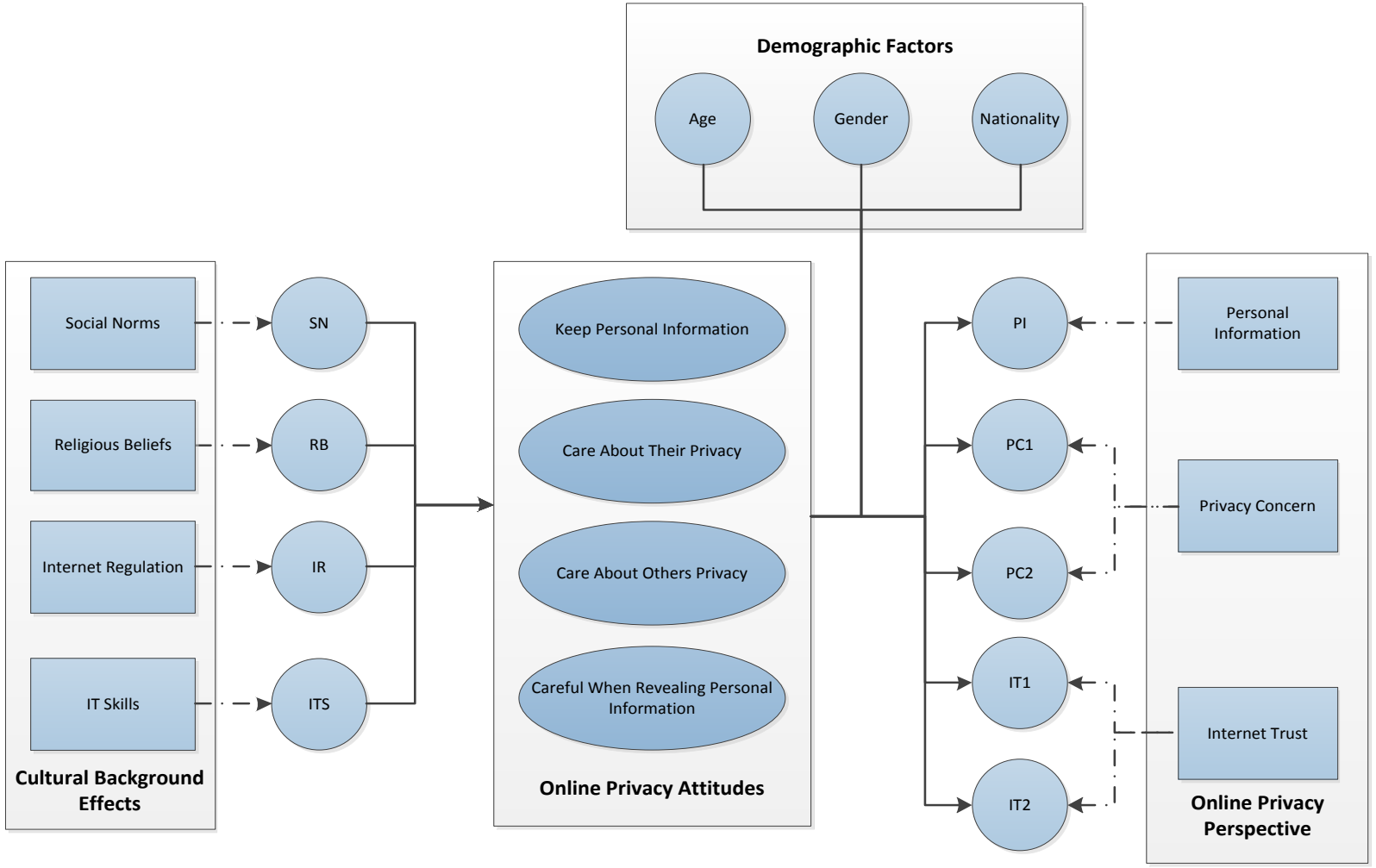


Figure 5-7: The Final Research Model

5.6 RESEARCH INSTRUMENT

This research investigates the relationship between the individual's online privacy perspective and the effects of cultural background on online privacy attitudes which are represented on the research model (see section 5.2). These relationships were examined using a questionnaire with a five-point scale designed to gather data on the relevant constructs. These constructs were online personal information, online privacy concerns, online trust, the safety of online information exchange and concerns over the possible secondary usage of personal information. In addition, the following constructs were also examined via the questionnaire, the effect of social norms on online privacy attitudes, the effect of religious beliefs on online privacy attitudes, the effect of Internet regulation on online privacy attitudes and the effect of IT skills on online privacy attitudes. These constructs were selected from validated items from previous studies of Internet privacy concerns (Table 5.1). In addition, supplementary data was collected on Internet experience, amount and level of Internet usage and other demographic characteristics, including gender, age, level of education and occupation. Section 5.6.1 gives further details of the constructs and questions of the questionnaire.

5.6.1 RESEARCH CONSTRUCTS AND QUESTIONS

Questions for gathering data on what constitutes online personal information were developed from the literature review (Smith *et al.*, 1996; Dinev and Hart, 2003). Questions for gathering data on online privacy concerns, online trust, the safety of online information exchange and concern for the possible secondary usage of personal information were adapted from Dinev and Hart (2006), and Xu *et al.* (2008). Questions on the effects of social norms and on online privacy attitudes were adopted from Xu *et*

al. (2008). Questions about other cultural effects, for example, the effect on online privacy attitudes of religious beliefs, IT skills and Internet regulation are modified from Xe *et al.* (2008). Questions on the level of Internet usage were adopted from Dinev and Hart (2003).

5.6.2 THE QUESTIONNAIRE

The questionnaire was divided into six groups of questions designed to take approximately 20 minutes to answer. The first three groups of questions were designed to provide a number of statements in relation to each dependent and independent variable, which are mentioned in (section 5.3: Research Variables and Hypotheses). Each statement is followed by a "five points Likert" scale includes five levels of agreement; 1. Strongly disagree, 2. Disagree, 3. Neither agrees nor disagree, 4. Agree, 5. Strongly agree (Gliem and Gliem, 2003, p.82)

The middle three levels of agreement (agree, disagree or neither agree or disagree) provide a sufficient number of options for the participants to express their opinion regarding each statement. The two extremes level of agreements (strongly disagree and strongly agrees) provide an opportunity for the participants to express any differences in the level of disagreement or agreement with regard to more than one statement (Garland, 1991, p.2).

The following section provides a detailed outline of each group of questions (See appendix B).

5.6.2.1 First group of questions: Personal Information Online

For the first group of questions, participants were provided with a definition of privacy online as, 'control of personal information while using the Internet'. The participants were asked to identify what they consider personal information when using the Internet (PI), based on the four categories of online personal information that have been mentioned in section two (2.4.1). These categories of online personal information are personal data, such as, name, address, telephone number and e-mail address; sensitive data, such as, religion, nationality and political opinion; identification data, such as, identification card number and DNA and anonymous data, such as, gender and age (Guarda and Zannone, 2008, p.7 and Ghani and Sidek, 2009, p.411). In order to answer this group of questions, which started with the question "What is personal information to you when you are using the Internet?" the participants were provided with a list of 11 items of information from the four categories mentioned above and asked to indicate their level of agreement using the five point Likert scale mentioned above.

The statement was, "When I am using the Internet, I consider the following information about myself personal information.", and the 11 items of information were, First name, Full name, E-mail address, Home address, Phone number, Date of birth, Photographic image, Credit card number, Nationality, Religion, and Political views (Smith *et al*, 1996 and Dinev and Hart, 2003).

This variable and its attendant questions were included in the questionnaire for two reasons. Firstly, to prepare the participants for the ensuing questions and place them into a relevant mindset about what this research means by the term 'personal information' as

illustrated by one or more of the 11 items mentioned above. Secondly, to investigate the similarities and differences between Malaysian and Saudi participants with regard to what they consider to be personal information (Smith *et al.*, 1996 and Dinev and Hart, 2003).

5.6.2.2 Second group of questions: Online Privacy Concerns and Trust

The second group of questions were divided into four sub-groups. The first sub-group of questions dealt with online privacy concerns when submitting personal information online (PC1). For this sub-group of questions about the "level of concern about submitting personal information online to 11 types of Internet website", the participants were asked to indicate their level of agreement (using the above mentioned 5 point Likert scale) to the concern they felt while submitting personal information via the 11 types of Internet website. The statement was, "When I am using the Internet, I am concerned about submitting personal information via: 1) e-mails, 2) search engines, 3) social networking websites, 4) newspaper websites, 5) instant messaging services websites (i.e. using Messenger), 6) online games websites, 7) video sharing websites (i.e. YouTube), 8) live TV and radio websites, 9) e-commerce websites (i.e. to purchase goods or services), 10) online banking websites, 11) e-Government websites.", (Dinev and Hart, 2006, and Xu *et al*, 2008).

The second sub-group of questions was about online privacy trust when submitting personal information online (IT1). For this sub-group of questions, the participants were asked to indicate their level of agreement about their trust with regard to handling personal information online by 11 types of Internet website. The statment was, "I believe that my personal information is handled in a professional way when I submit it

via 1) e-mails, 2) search engines, 3) social networking websites, 4) newspaper websites, 5) instant messaging services websites (i.e. using Messenger) , 6) online games websites, 7) video sharing websites (i.e. YouTube) , 8) live TV and radio websites, 9) e-commerce websites (i.e. to purchase goods or services), 10) online banking websites, 11) e-government websites", (Dinev and Hart, 2006, and Xu *et al*, 2008).

The third sub-group of questions was about safety when exchanging personal information online (IT2). For this sub-group of questions, the participants were asked to indicate their level of agreement about their level of trust with regard to safety when exchanging personal information with others on six types of Internet websites. The statement is, "I believe that it is safe to exchange information with others using 1) e-mails, 2) social networking websites, 3) newspaper websites, 4) instant messaging services websites (i.e. using Messenger), 5) online games websites, 6) video sharing websites (i.e. YouTube)", (Dinev and Hart, 2006, and Xu *et al*, 2008).

The Fourth sub-group of questions was about online concerns with regard to the destiny of personal information submitted online (PC2). For this sub-group of questions, the participants were asked to indicate their level of agreement with their level of concern with regard to the destiny of the personal information submitted online. The statment was, "I am concerned that the information I submit on the Internet could 1) be misused, 2) be found by others, 3) be used by others, 4) be used in a way I did not expect, 5) be used in a way I am not comfortable with, 6) be used in a way that could threaten my security, 7) be used in a way that invades my privacy, 8) be used in a way that could create unexpected problems" (Dinev and Hart, 2006, and Xu *et al*, 2008).

5.6.2.3 Third group of questions: the role of culture, religion, technological and regulatory effects

For the third group of questions, the participants were asked to indicate their level of agreement using the above-mentioned five point Likert scale to indicate the level of the effect of their social norms, religious beliefs, IT skills and Internet regulation on their privacy attitudes (Table 5.3). This group of questions included the following 16 statements:

1. Keeping my personal information is very important according to my friends and family.
2. Keeping my personal information safe is very important based on my religious beliefs.
3. Keeping my personal information safe is very important according to the Internet regulations in my country.
4. Keeping my personal information safe is very important based on my IT skills.
5. I should care about my privacy according to my friends and family.
6. I should care about my privacy based on my religious beliefs.
7. I should care about my privacy according to the Internet regulations in my country.
8. I should care about my privacy based on my IT skills.
9. I should care about others' privacy according to my friends and family.
10. I should care about others' privacy based on my religious beliefs.
11. I should care about others' privacy according to the Internet regulations in my country.
12. I should care about others' privacy based on my IT skills.

13. I should be careful when revealing personal information according to my friends and family.
14. I should be careful when revealing personal information based on my religious beliefs.
15. I should be careful when revealing personal information based on the Internet regulations in my country.
16. I should be careful when revealing personal information based on my IT skills,

Table 5-3: Independent Variables and their related questions in the questionnaire (each question was designed to indicate the level of agreement using 5-point Likert scale for each item of each variable)

Variables	Statements* *Each question has been designed to indicate the level of agreement (using 5 Likert scale) on one statement as follows:	References
Religious Beliefs Effect (RB)	1) Keeping my personal information safe is very important, based on my religious beliefs 2) I should care about my privacy based on my religious beliefs 3) I should care about others' privacy based on my religious beliefs 4) I should be careful when revealing my personal information based on my religious beliefs	Ballman *et al.*, 2004, Dinev *et al.*, 2005, Siala *et al.*, 2004, and Xe *et al.*, 2008
Social Norms Effect (SN)	1) Keeping my personal information safe is very important, based on my friends and family 2) I should care about my privacy based on my friends and family 3) I should care about others' privacy based on my friends and family 4) I should be careful when revealing my personal information based on my friends and family	
Internet Regulation Effect (IR)	1) Keeping my personal information safe is very important, based on Internet Regulation in my country 2) I should care about my privacy based on Internet Regulations in my country 3) I should care about others' privacy based on Internet Regulations in my country 4) I should be careful when revealing my personal information based on Internet Regulations in my country	Ballman *et al.*, 2004 and Dinev and Hart, 2006
IT Skills Effect (RB)	1) Keeping my personal information safe is very important, based on my IT Skills 2) I should care about my privacy based on my IT Skills 3) I should care about others' privacy based on my IT Skills 4) I should be careful when revealing my personal information based on my IT Skills	Milberg *et al.*, 2000, and Wirtz *et al.*, 2006, pp. 340-341

5.6.2.4 Fourth and fifth groups of questions: the level of internet usage

For the fourth and fifth groups of questions, the participants were asked to provide information about their Internet usage. These included the number of hours spent per week on the Internet, the number of years using the Internet, the places where they use

the Internet and their level of usage for the 11 Internet activities; 1) e-mails, 2) search engines, 3) social networking websites, 4) newspaper websites, 5) instant messaging services websites (i.e. using Messenger), 6) online games websites, 7) video sharing websites (i.e. YouTube) , 8) live TV and radio websites, 9) e-commerce websites (i.e. to purchase goods or services), 10) online banking websites, 11) e-government websites. With regard to the level of Internet usage for the above mentioned 11 Internet activities, participants were asked to use the following scale to identify their level of usages; (1.Never, 2. Once or a few times in my life, 3. Once, or twice a month, 4. At least once a week, 5. Almost every day).

5.6.2.5 Sixth group of questions: General information about yourself

Finally, for the sixth group of questions, the participants were asked to provide more demographic information including their age, gender, level of education, occupation, religion, nationality and ethnic background. The information about age, gender and nationality would be used as a part of the research investigation, i.e. the demographic factors (see section 5.3). The demographic information is collected in order to provide a description of the targeted participants, which will help in the explanation of the results, for example to see if there are differences between nationality, age or gender groups (Fink, 2003 pp. 79-84) and to help the selection of those who are fallen in the target participants that are described in section (5.7.1: Target Participants).

The demographic information was sought from the sixth (last) group, because some of the demographic questions might be sensitive, eg. asking about age and religion, therefore, they should be placed at the end of the questionnaire to prevent any negative effect on the willingness of participants to answer the other questions due to the feeling

of a loss of the anonymity that the demographic questions may cause (Oppenheim, 1992, p. 109 , and Lietz, 2010, p. 257) Another reason for putting the demographic questions at the end of the questionnaire is to focus on their full attention at the beginning of the questionnaire in answering the main questions that needed more thought.

5.6.3 PILOTING THE QUESTIONNAIRE

Piloting a questionnaire is an essential part of research procedure. For example, Vaus (2002, pp. 52-54) argues that having designed the research instrument and before starting to collect data it is sensible to evaluate the validity and reliability of the research instrument to avoid or minimise any measurement error. In addition, Ruane (2005, pp.32-42) states that although a good research procedure tends to protect against research design errors it is possible to find errors in the findings which may be due to unclear evidence or biased samples. To ensure the validity of the findings one needs to concentrate on three trust issues in the research instruments, that is, trust in the questionnaire's claims of measurement (measurement validity), in the causal statement (internal validity) and in the findings (external validity). Furthermore, Sarantakos (2005, pp.254-256) states that validity is critical to pre-test and pilot instruments before starting to collect data in quantitative research. This is to ensure the reliability and validity of both the organisation and items of such data collection instruments.

Prior to the start of the data collection for this research, two pre-tests were conducted. First, the validity of the questionnaire was tested to ensure that the questionnaire's items would measure the relevant concepts they were intended to measure. Second, the

reliability of the questionnaire was tested to ensure that participants would answer the questions in the same way every time the questions were asked (Vaus, 2002, pp.52-54, Bryman, 2008, pp.149-154).

In this research, the validity test was performed using a cognitive interview (Jobe and Mingay, 1991, pp.1053-1055; DeMaio *et al*, 1998, pp.50-51; Presser *et al.*, 2004, pp.109-112) at the pilot stage, i.e. before collecting the data (see section 5.6.3.1), and using factor analysis (Premkumar and Ramamurthy, 1995, p.318, and Zeller and Carmines, 1980, p.84) at the data analysis stage, i.e. after collecting the data (see section 6.2.4.2). The reliability test was conducted using Cronbach's Alpha Test (Vaus, 2002, pp.52-54; Straub *et al.*, 2004, p.385) before and after collecting the data (see sections 5.6.3.2 and 6.2.4.1). The validity and reliability test on the pilot stage are described in details at the following sections, 5.6.3.1 and 5.6.3.2.

5.6.3.1 Cognitive interview as a validity test

The questionnaire was examined with regard to the clarity of its structure and questions by a technique called "cognitive interview." The aim of the cognitive interview is to identify any confusion or problems that the questionnaire may contain as well as to find out the reasons for these problems. The cognitive interview is derived from the cognitive sciences and is a technique for examining the clarity of the survey's process in terms of its language and perception. Such examination would enable the measurement of possible errors that could occur due to the participant's misunderstanding of the survey (Campanelli, 1997, p.5). Therefore, a cognitive interview aims to provide a simulation of the expected processes and outcomes of the questionnaire's items (Presser *et al.*, 2004, p.111).

Participation in the cognitive interviews involved an hour long (voice recorded) interview, starting with reading aloud and answering the questionnaire (Campanelli, 1997, p.7), then answering some probing questions in order to identify the participants' views regarding the wording and the structure of the questionnaire (Campanelli, 1997, p.8). During the cognitive interviews, participants were asked to say whatever came into their minds while they read and answered the questions via a process called 'thinking out loud' (Campanelli, 1997, pp.7-8). To familiarise the participant with the cognitive interview procedure the researcher gave a practical training example of the 'thinking out loud' technique by answering this question, "'How many windows are there in your house?' If I was thinking out loud, I would say, 'Well, there are three windows in the living room, another three in my daughter's bedroom and another three in my bedroom, so I have 9 windows'" (Campanelli, 1997, p.8). Appendix C includes the main outcomes of the cognitive interviews that include the main points that were highlighted during the 'thinking out loud' process with regard to the wording and the structure of the questionnaire.

During the second part of the cognitive interviews and following the 'thinking out loud' exercise participants were asked some probing questions, which consisted of both pre-determined and spontaneous questions which could be developed during the interview (Willis, 1994, from (Campanelli, 1997, p.8). As a result of the cognitive interviews, a number of changes were made to the questionnaire items (see Appendix C). The outcome of the cognitive interviews informed the final version of the questionnaire.

5.6.3.2 Cronbach's Alpha as a reliability test

Cronbach's Alpha is a common test for evaluating reliability. It calculates coefficient reliability (Bryman, 2008, p.151), which assesses internal consistency (Bland and Altman, 1997, p.572) by measuring the inter-correlations between the questionnaire's items. To evaluate the questionnaire's reliability a small-scale collection of data using 38 questionnaires was conducted. The participants for this reliability test were Saudi students studying at De Montfort and Leicester universities. The data was coded and entered into an SPSS file. A Cronbach's Alpha test was performed upon the data using the statistical software and a result of 0.710 was obtained, which indicates 'a satisfactory level' of reliability (Bryman, 2008, p.151).

5.7 POPULATION AND PARTICIPANTS

In order to accomplish the objective of this comparative study the population selected for the research consisted of Muslim students and members of staff at higher education establishments from the two Islamic countries, Saudi Arabia and Malaysia 2.5 The Study Context). In the following subsection the characteristics of the target participants, the sampling process for their selection and the data collection strategy are described.

5.7.1 TARGET PARTICIPANTS

This research is interested in identifying the cultural effects, which include those of social norms, effect of religious belief, IT skills and Internet regulation on online privacy and comparing these effects within two cultural backgrounds, namely, Saudi Arabia and Malaysia. For this purpose, the researcher was interested in the effect of religious beliefs within different cultural backgrounds, not in the effects of different religions. The target participants, therefore, needed to be from one religion, i.e. Islam,

which is the main religion of the target countries. In addition, to maintain a relatively reasonable level of IT skills and knowledge of Internet regulation among the target participant rather than have results observed by variation in such knowledge, the researcher selected members from higher education i.e. students and members of staff from universities. Thus, the common characteristics of the target participants for this research were set to be Muslims (students or members of staff) at any Malaysian, or Saudi Arabian University at the time of this research.

5.7.2 POPULATION AND SAMPLING

As it is difficult, if not impossible, to collect data from everyone in the investigated population, data was collected from a representative sample (Denscombe, 2010, p.11).

The sampling process was divided into two stages. In the first stage, a stratified sampling technique was used to make sure that each member of the population had the same chance of being selected according to their proportion. A total sample size of 878 participants was used with 515 participants (60%) from Saudi Arabia and 336 participants (40%) from Malaysia. These two samples reflected approximately the same percentage of their country's Muslim population (Table 5.5).

Table 5-4: The total population and number of participants

Members of the Population	Muslim Population	Sample Size	Sample Proportion
Saudi Arabia	26,131,703	515	0.0020%
Malaysia	17,347,246	363	0.0021%

In the second stage, a cluster sampling technique was applied to each member of the population. In cluster sampling, groups, i.e. geographic areas from each country (Table 5.6) are selected and then a random sampling technique is applied to these groups to ensure that the balance between the groups or cluster samples and the entire population prevents non-representative samples. A representative sample is very important to enable the generalisation of the findings to the whole population (Denscombe, 2010, p..22).

Table 5-5: The clusters/groups from the two members of the population

Saudi Arabia		Malaysia	
University	**City**	**University**	**City**
King Saud	Riyadh	Utara Malaysia	Kedah
King Abdul-Aziz	Jeddah	Sains Malaysia	Penang
Taif	Taif	Teknologi Mara	Kuala Lumpur
Um al Quara	Makkah	Kebangsaan Malaysia	Kuala Lumpur
King Fahad	Dhahran		

5.7.3 DATA COLLECTION

Participation in this research involved completing an eight-page questionnaire (see Appendix B). The questionnaires were distributed by hand and retrieved at a "drop off/pick up" point, a technique used to avoid the non-response problems associated with postal questionnaires (Steele, *et al*, 2001, p.239). The data collection in this research was conducted by the researcher himself and a number of research assistants who were either one of the students or members of staff from the targeted universities. The research assistants helped voluntarily, in their free time, to access the targeted participants at some of the universities involved. Using this technique, the researcher

and research assistants distributed the questionnaires before or at the end of lectures or meetings and then collected them back later at the same lectures or meetings or at subsequent ones.

The researcher or the research assistant clarified the participants' rights, which included their right to refuse any of the questions and to withdraw from the study at any time by advising the researcher. Appendix D includes the full letter explaining consent given to the participants, and the guideline for the volunteer research assistants, on how to distribute and collect the questionnaire, including the ethical and procedural issues that needed to be considered as they conducted the data collection.

5.7.4 CONCLUSION

This chapter discussed, mainly, the design and validation of the questionnaire instrument, its translation and the data collection process. In the design of the questionnaire, the six groups of questions of the questionnaire were illustrated with the connection to their relevant independent and dependent variables. Then the process of translation and piloting and validation of the questionnaire including the use of the cognitive interviews as the validity test and Cronbach's Alpha as the reliability test were discussed. Finally the protocol of the data collection from the relevant participants including the population and sampling and the process of the data collection were explained. In the following chapter, the descriptive data analysis as a part of the research findings which have been collected from both Saudi Arabian and Malaysian participants is discussed in details.

6 CHAPTER 6: DESCRIPTIVE DATA ANALYSIS

6.1 INTRODUCTION

Previous chapters have discussed the research's methodology and design in detail. In Chapter 5, the research aim, questions, variables and hypotheses were described, including the questionnaire's design, validation, translation and data collection.

The purpose of this study is to investigate the relationship between privacy concerns and the Internet and how they are affected by an individual's cultural surroundings. The research, therefore, has been designed to identify a) cultural influences that affect the privacy perspectives of individual Muslims in their internet usage and b) identify similarities and differences between the perspectives of individual Muslims from different cultural backgrounds. To investigate these issues, various data about the participants needed to be collected and analysed. The data included demographic characteristics, Internet usage and activities, levels of online privacy concerns and trust, the effects of religious beliefs, IT skills, family, friends and Internet regulation on the online privacy attitude.

This chapter describes the analytical methods used on the descriptive data collected from both Saudi Arabian and Malaysian participants. The chapter will start by providing a data screening assessment for the collected data with regard to outliers and normality in order to satisfy the requirements of the regression assumption presented in the next chapter as part of the inferential data analysis. Next, the chapter will assess whether the questionnaires have reached the required levels of reliability and validity prior to any data analysis. This is followed by a description of the demographic characteristics of the participants from both countries before moving on to describe their Internet usage and

activity. Following this, the level of online privacy concerns and trust, effects of religious beliefs, IT skills, family, friends and Internet regulations on online privacy attitudes will be reported.

6.2 RESEARCH POPULATION AND SCREENING DATA FOR THE ANALYSIS

The population studied in this research are Muslim students and members of staff in higher education from Saudi Arabia and Malaysia. To target this population, a total sample size of 878 individuals was used of which 515 participants (60%) came from Saudi Arabia and 363 (40%) from Malaysia, which approximately represents the same proportion of the Muslim population in each country (see Table 5.5, Chapter 5).

Using a cluster sampling technique, a number of universities from each country (see Table 5.3, chapter 5) were selected as cluster groups to ensure a balance between the representations of the geographic areas covered by the entire population and, therefore, reduce the chance of non-representative samples.

In order to prepare the data for the descriptive and inferential data analyses, researchers need to screen the data for accuracy and for outliers within cases (Tabachnick and Fidell, 2007, p60). Subsections (6.2.1) and (6.2.2) include details on the importance and the procedures involved the accuracy and outliers tests (Table 6.1).

Table 6-1: Data screening tests

Data Screening Test	Description
Check the accuracy	Proofread the original data against the computerised data file
Find the outliers	Find any observations that are very different from others which could statistically bias the mean

6.2.1 CHECK FOR ACCURACY

It is essential, after entering the collected data into the statistic analysis programme (SPSS) and prior to starting the analysis to check the data for errors. For example, entering a number that is outside the possible range of values, such as inputting 33 instead of 3 in a range that is defined to be from 1 to 5. Checking of accuracy and cleaning the data is divided into two steps, the first is checking for errors and the second is their correction (Pallant, 2007, p.34).

In the checking for errors, the values of each variable are checked to ensure that they do not fall outside the range of possible values. For example, if the researcher defines the values of the gender variable as 0 for male and 1 for female, the only possible values that should be found for this variable are 0 and 1 and any other is considered as an error. Another example is if the values of a variable are defined on a scale of 1 to 5, any other value except 1,2,3,4 and 5 are considered an error. To check for such errors, a frequent table for each variable including the minimum and maximum values are checked using the SPSS programme. Any variables with minimum and maximum values that fall outside the defined range are considered erroneous. In correcting errors, values of the variables that are identified with error are sorted as ascending and/or descending (depending on whether the error data are above and/or below the range of defined values of the variable), then any data outside the defined values are removed.

6.2.2 TEST THE OUTLIERS

An outlier is a case with an extreme value on one variable, a “uni-variable outlier” or two or more variables, a “multivariable outlier” (Field, 2009, p.102). This could happen

for a number of reasons and either the researcher or the participants could cause it. It could occur due to incorrect data entry or problems with regard to specifying missing values by the researcher. Alternatively it could happen because the participants fall outside the target population or they are unable or do not want to decide which level of scale to select (Bryman, 2008, p.325; Field, 2009, p.102; Tabachnick and Fidell, 2007, pp.72-73, Howell, 2010, p.21)**.**

Outliers could be considered either a problematic or a beneficial characteristic in the data. For example, outliers could be an indication of the existence of a unique characteristic group within the data, which could be considered as a discovery of a group that could not be revealed by using the normal data analysis procedures, such as, the correlation and other multivariate data analysis tests. It simply, however, could be a result of non-representative samples, which could deform the statistical tests (Hair *et al*, 1998, p.64).

Researchers, therefore, should view the outliers within the contexts of the data analysis to understand why they have occurred and whether they are problematic or beneficial. Hair *et al*, (1998, pp.64-65) placed the outlier into four classes. The first class of the outlier is the procedural error outlier, which could happen in the data entry stage and it could be identified and removed during the data cleaning stage. The second class is the observational outlier, which could arise because of an extraordinary event that is capable of being justified, for example, it could be an observation of a unique group of the population in which the researchers have an explanation for the uniqueness of these observations.

Researchers in this case and based on their judgment of the whole data could either decide to keep this outlier and consider it as a representative group of the sample or delete it. The third class is the same as the second class of the outlier in which they have a unique characteristic but with little or no explanation for this uniqueness. The outlier, in this case, is most likely to be deleted by the researchers unless they feel that the outlier represents a valid part of the population. The fourth class of the outliers is those with cases within the ordinary range of values but with a different combination value of the variables. In this case, the researchers must keep the outlier unless they have evidence to confirm that these cases are not a representative part of the population

An outlier could cause a statistical bias, for example, in both the mean and the regression coefficients. Outliers can be detected using a number of different techniques, for example, by calculating either the mean using the standard deviation (SD) around the mean or the z-score (Bryman, 2008, p.325; Field, 2009, p.102; Tabachnick and Fidell, 2007, pp.72-73). With regard to the mean and SD technique, the outlier can be identified using the 'rule of thumb', which looks at the value of the SD and identifies extreme values (Bryman, 2008, p.325). For the z-score, the outlier can be identified by looking at the percentages of specific values (Table 6.16) that aid the researcher in judging them (Field, 2009, p.103). These are the main techniques for testing outliers particularly if the researcher is interested in multi-variance outliers and plans to use factor analysis and regression (Tabachnick and Fidell, 2007, pp.72-73). In this research, both techniques have been used to identify outliers.

6.2.2.1 Mean and Standard Deviation (SD) technique

As mentioned above, the mean and SD is a technique for identifying if there are any outlier cases in the research sample. It is conducted by calculating the mean and SD for all the variables and looking for any extreme values as a 'rule of thumb' indication for the outlier within the cases (Bryman, 2008, p.325). The mean and SD values (Tables 6.2) did not indicate any outliers within either the Saudi or Malaysian samples. In order, however, to ensure that the samples are free from outlier cases the z-score technique was used as a further outlier test (see section 6.7.1.2).

Table 6-2: Mean and Standard Deviations for Saudi and Malaysian Samples

	Variables Code	Variables Name	Saudi Arabia		Malaysia	
			Mean	SD	Mean	SD
1	PI	Personal Information	3.16	0.39	3.30	0.42
2	PC-1	Internet Privacy Concern 1	3.03	0.48	3.33	0.48
3	PC-2	Internet Privacy Concern 2	3.55	0.688	3.69	0.51
4	IT-1	Internet Trust 1	2.99	0.48	3.09	0.49
5	IT-2	Internet Trust 2	2.73	0.58	2.95	0.53
6	SN	Social Norms	3.48	0.62	2.86	0.29
7	RB	Religious Beliefs	3.60	0.54	3.71	0.43
8	IR	Internet Regulation	3.30	0.63	3.57	0.49
9	ITS	IT Skills	3.40	0.61	3.57	0.53

6.2.2.2 Z-score technique

To ensure the accuracy of the outlier results z-score tests were conducted. The z-score is calculated by taking each case/observation, subtracting it from the mean and dividing the result by their SD. This creates a new distribution with a mean of zero and an SD of

1. In order to identify the outliers, the researcher scans the z-score of each observation and if there are either 95% or more observations with a z-score of 1.96 or less, 1% or less with z-score of 2.58 or 0% with z-score of 3.29 (Table 6.3) it can be concluded that there are no outliers (Field, 2009, p.103). Otherwise the test will have identified some outliers in the sample.

Table 6-3: Values of z-score and their maximum percentage to reject the outlier

Absolute Z-score	Valid Present of each Variable within the Sample
Less than 1.96	≤ 95%
Greater than 2.58	≤1%
Greater than 3.29	≤ 0%

In this research and as a rule of thumb, the third criteria, i.e. 0% of a 3.29 Z-score is adopted. The outliers in these samples were calculated using the SPSS software. The summary of the results, with the valid percentage for each possible z-score are illustrated in Table 6.4, with highlighting those relevant to the selected criteria (0% of a 3.29 Z-score). The table shows that the Saudi and Malaysian samples have respectively 6 variables (PC-2, IT-1, SN, RB, IR and ITS) respectively and 5 variables (PC-2, SN, RB, IR and ITS) with one or more outliers.

Table 6-4: Values of z-score and their maximum percentage to reject the outlier for the Saudi and Malaysian samples

	Variables Code	% of Absolute Z-score							
		Saudi Arabia				Malaysia			
		<1.96	>1.96	>2.58	>3.29	<1.96	>1.96	>2.58	>3.29
1	PI	97.0	2.2	0.8	0	96.8	2.3	0.9	0
2	PC-1	96.5	3.5	0	0	96.6	3.1	0.3	0
3	PC-2	89.6	10.4	0	0	93.8	1.4	3.9	1.9
4	IT-1	92.6	7.4	0	0.2	97.0	3.0	0	0
5	IT-2	95.3	4.7	0	0	100	0	0	0
6	SN	90.7	9.3	0	0	92.7	3.9	1.9	1.5
7	RB	91.4	4.9	3.7	0	95.8	1.7	1.1	1.4
8	IR	93.0	7.0	0	0	95.0	2.2	2.8	0
9	ITS	94.4	5.6	0	0	93.7	6.3	0	0

In order to deal with the identified outliers three points have been considered as follows. The first point is that the data collection was conducted in person by the researcher using a hand delivery and retrieve (drop off/pick up) technique (see section 5.7.3) in order to ensure the correct selection of the target participants. The second point is that the researcher himself did the data entry in a very careful manner with a well-established missing value procedure. The third point is that the screening of the outliers for each variable in both the Saudi and Malaysian samples, which was done by the researcher, concluded that there is no evidence of any common characteristics among cases within each outlier. In other words, these cases are not from a specific gender, age, level of education or Internet usage. Therefore, the most likely reason proposed by the researcher was that some of the participants did not complete the questionnaire with

a reasonable level of reliability. This could be due to either a lack of interest in the study or an interruption during the process of filling in the questionnaire. Such a conclusion would support the third class of outliers as explained earlier in this section, which suggests that they are the results of extraordinary events of observations with no explanation for their occurrence (Hair *et al*, 1998, pp.64-65). Consequently, it is important to highlight that both Saudi and Malaysian samples are relatively biased with regard to the outlier result. Hence, it is essential dispense with those cases that caused outliers on the variables.

In order to drop the outliers the z-scores of each variable that were identified as having them are sorted ascending order by the SPSS file and then all the relevant cases, i.e. those with z-scores above the valid value mentioned in (Table 6.3) are dropped. The detailed process of dropping the outlier cases for both the Saudi and Malaysian samples is illustrated in tables 6.5 and 6.6 respectively.

Table 6-5: The process of deleting the outlier cases in the Saudi Sample

	Variables Code	Description	Dropped cases	Remained cases
1	PI	Do not need to remove any cases as there are no outliers (0% of a 3.29 Z-score)	0	515
2	PC-1	Do not need to remove any cases as there are no outliers (0% of a 3.29 Z-score)	0	515
3	PC-2	Do not need to remove any cases as there are no outliers (0% of a 3.29 Z-score)	0	515
4	IT-1	1 case (0.2%) that has a 5.43 Z-score was removed	1	514
5	IT-2	Do not need to remove any cases as there are no outliers (0% of a 3.29 Z)	0	514
6	SN	Do not need to remove any cases as there are no outliers (0% of a 3.29 Z)	0	514
7	RB	Do not need to remove any cases as there are no outliers (0% of a 3.29 Z)	0	514
8	IR	Do not need to remove any cases as there are no outliers (0% of a 3.29 Z)	0	514
9	ITS	Do not need to remove any cases as there are no outliers (0% of a 3.29 Z)	0	514

Table 6-6: The process of deleting the outlier cases in the Malaysian Sample

	Variables Code	Description	Dropped cases	Remained cases
1	PI	Do not need to remove any cases as there are no outliers (0% of a 3.29 Z)	0	363
2	PC-1	Do not need to remove any cases as there are no outliers (0% of a 3.29 Z)	0	363
3	PC-2	3 cases were deleted in order to reduce the percentage of cases that have a z-score of more than 3.29 from 1.9% to the acceptable percentage of 0%.	3	360
4	IT-1	Do not need to remove any cases as there are no outliers (0% of a 3.29 Z)	0	363
5	IT-2	Do not need to remove any cases as there are no outliers (0% of a 3.29 Z)	0	363
6	SN	2 cases were deleted in order to reduce the percentage of cases that have a z-score of more than 3.29 from 1.5% to the acceptable percentage of 0%.	2	358
7	RB	A further 1 case was deleted in order to reduce the percentage of cases that have a z-score of more than 3.29 from 1.4% to the acceptable percentage of 0%.	3	357
8	IR	Do not need to remove any cases as there are no outliers (0% of a 3.29 Z)	0	357
9	ITS	Do not need to remove any cases as there are no outliers (0% of a 3.29 Z)	0	357

Because of the outlier deletions, the number of individuals sample retained for this research was reduced from the original total of 878 to 871 participants of which 514 were from Saudi Arabia and 357 were from Malaysia.

6.2.3 TEST THE NORMALITY

Normality is the degree to which the distribution of the sample data corresponds to a normal distribution (Hair *et al.*, 1998, p.38). Screening continuous variables for normality is an important early step in almost every multivariate analysis, particularly

when the goal is inference. The rationale behind hypothesis testing relies on having data that is normally distributed. Therefore, if this assumption is not met then the logic behind hypothesis testing will not be valid (Tabachnick and Fidell, 2007, p.79**).** Field (2009, pp.155-156) argues that a bigger sample provides more confidence on the normality of its distribution. He added that a number of researchers believe that most samples with more than 40 cases could be predicted to be normally distributed. With regard to the Saudi and Malaysian samples, they consist of 473 and 333 cases respectively, thus according to Field's argument there should be no problem in assuming the normality of both samples. In order, however, to provide statistic evidence for the normality, the researcher conducted a normality assessment for all the research's variables.

The normality of the variables is assessed by either statistical or graphical methods. A simple test is a rule of thumb based on the skewness and kurtosis value (Hair *et al.*, 1998, pp.71-73). The perfectly normally distributed sample should have a zero value for both skewness and kurtosis, which is not normally the case in social studies. Values above or under the zero value indicate the shape of the sample distribution (Table 6.7). For example, positive values of skewness indicate a high number of low scores in the sample distribution whereas negative values point out that there are more high scores in the sample. On the other hand, positive values of the kurtosis result in a pointy and heavily tailed sample distribution whereas negative values produce a flat and light-tailed distributed sample with the maximum acceptance value of (+/-3.29) for both Skewness and Kurtosis (Field, 2009, p.139).

Table 6-7: The indications of Skewness and Kurtosis values

	Values Direction	Direction Indication	0 Value Indication	Upper Threshold
skewness	**Positive**	high number of low scores on the sample distribution	Distribution is normal	+ 3.29
	Negative	there are more high scores on the sample		-3.29
kurtosis	**Positive**	pointy and heavily tailed sample distribution	Distribution is symmetric	+ 3.29
	Negative	a flat and light-tailed distributed sample		- 3.29

Table 6.8 illustrates the skewness and kurtosis values for the Saudi and Malaysian samples. The table shows that skewness and kurtosis values are within the acceptance values of (+/-3.29) for both Skewness and Kurtosis.

With regard to the Malaysian sample, it can be seen from table (6.8) the RB (i.e. the independent variable for the effect of religious belief on the online privacy attitude) records the highest value of Skewness (-1.56) and Kurtosis (1.5). This indicated that this variable has more high scores (4 and 5 out of 5), which made the distribution curve pointy and heavily tailed. This suggests there are a high number of participants who agree and strongly agree with the effect of religious beliefs on the online privacy attitude (Appendix E).

With regard to the Saudi sample, table (6.8) shows that the SN (i.e. the independent variable for the affect of social norms on the online privacy attitude) records the highest value of Skewness (-2.97) and Kurtosis (1.26). This indicated that this variable also has more high scores (4 and 5 out of 5), which made the distribution carve pointy and

heavily tailed. This suggests there are a high number of participants who agree and strongly agree with the effect of social norms on the online privacy attitude (Appendix E).

Table 6-8: Normality assessment for Malaysian and Saudi Arabian samples

	Variables	Malaysian		Saudi Arabian	
		Skewness	Kurtosis	Skewness	Kurtosis
1	PI	- 0.10	- 0.15	- 0.23	- 0.34
2	PC-1	- 0.01	- 0.64	- 0.37	- 0.70
3	PC-2	- 1.37	0.28	- 1.95	2.91
4	IT-1	0.01	- 0.48	- 0.22	- 0.61
5	IT-2	0.46	- 0.65	- 0.03	- 0.71
6	SN	- 1.12	0.11	- 2.97	1.26
7	RB	- 1.56	1.50	- 1.52	1.85
8	IR	- 0.715	- 0.579	- 1.04	0.38
9	ITS	- 0.798	- 0.398	- 1.19	0.75

6.2.4 RELIABILITY, VALIDITY AND FACTOR ANALYSIS TESTS

The research instruments that contain the items of the research's variables are designed to answer the research questions. In order to increase the confidence in these research instruments to ensure they are doing their jobs properly two important assessments need to be made, namely, the validity and reliability assessments. As mentioned in chapter five (section 5.6.3) validity assessment is used to test whether the research instruments are measuring what they are designed to measure whereas the reliability assessment is used to test whether these instruments are interpreted consistently across all cases, i.e. by the participants (Field, 2009, pp.11-12 and Zeller and Carmines, 1980, p.77). In the

following sections the detailed results of the reliability (section 6.3.1) and validity assessments and the factor analysis (section 6.3.2) are discussed.

6.2.4.1 Reliability Test

Using inter-item consistency (Cronbach's coefficient alpha), the reliability of the nine research's instruments (variables) were tested. A research instrument is considered as reliable if the value of its Cronbach's alpha is 0.7 or more (Field, 2009, p.681) or according to Hair et al (1998, p.118) and Nunnally (1967) more than 0.6. In addition, a value of more than 0.8 is considered a good level of reliability (Hair et al, 1998, p.118 and Field, 2009, p.681). Table 6.9 shows the results of the reliability (Cronbach's Alpha) test for both Saudi and Malaysian samples (Full details can be found in Appendix E (Tables 6.10 and 6.11). It is worth mentioning that some variables have a 'just about' acceptable level of reliability, for example, the Cronbach's Alpha value of the (PI) in Saudi Arabia is (0.659) and the value of the (SN) in Malaysia is (0.690). Cronbach's Alpha values for the rest of the variables are either acceptable or good.

Table 6-9: The reliability (Cronbach's Alpha) scores for each Variables for the Saudi and Malaysian Samples

Variables	No. of Items	Cronbach's Alpha	
		Saudi Arabia	Malaysia
PI	11	0.664	0.727
PC-1	11	0.782	0.845
PC-2	8	0.958	0.924
IT-1	11	0.805	0.868
IT-2	5	0.780	0.789
SN	4	0.823	0.580
RB	4	0.837	0.812
IR	4	0.847	0.835
ITS	4	0.857	0.877

6.2.4.2 Validity and Factor Analysis

Chapter five (section 5.6.3.1) discussed the validity test that pertained to the pilot stage. The test was conducted using the cognitive interview technique in order to identify any confusion or problems surrounding the structure and wording of the questions in the questionnaire. At this stage, i.e. after collecting the data using the final version of the questionnaire, factor analysis was used to test the validity of the items of the research's instruments (Premkumar and Ramamurthy, 1995, p.318, and Zeller and Carmines, 1980, p.84). The factor analysis aims to identify any correlations between the items of a research instrument and any latent (hidden) variables and so confirm or reject the relationship between the items of each research instrument (variable). In other words, the result of the factor analysis indicates whether each item of a research instrument measures what this instrument was designed to measure (Field, 2009, p.786, and Zeller and Carmines, 1980, p.77). In addition, to examine the adequacy of the research sampling, another test, the Kaiser-Mayer-Olkn (KMO, is used). The KMO value, which can be between zero and 1 indicates whether the correlations between the items of a variable are valid within the collected sample or not. KMO Values between 0.5 and 0.7 are acceptable, values between 0.7 and 0.8 are good and between 0.8 and 0.9 are excellent (Field, 2009, p.647).

The results of factor analysis and KMO as the validity measurement for both Saudi and Malaysian samples are summarised in Appendix E (tables 6.12 and 6.13). All the variables of the Saudi and Malaysian samples correlated to their items with good to excellent KMO values, therefore, the research instruments were found to be valid within the research samples.

6.3 DEMOGRAPHIC CHARACTERISTICS

As mentioned in Section 6.2, the research sample was reduced to 514 participants from Saudi Arabia and 357 from Malaysia.

The participants were asked to provide, upon the questionnaire, demographic information about themselves in terms of age, gender, level of education, occupation, religion, nationality and ethnic background. Table 6.10 summarises the demography of the participants.

Table 6-10: Demographic characteristics of the participants from Saudi Arabia and Malaysia

		Saudi Arabia		Malaysia	
Demographic Characteristics		Frequency	%	Frequency	%
Gender	**Male**	260	50.6	89	24.9
	Female	253	49.4	268	75.1
Age	**18-22**	333	64.8	280	78.4
	23-27	116	22.6	53	14.2
	28-32	21	4.0	9	2.4
	Over 32	44	8.6	15	5
Highest level of Education	**Undergraduate**	394	76.7	277	77.6
	Postgraduate	87	16.9	75	21.0
	PhD	33	6.8	5	1.4
Occupation	**Student**	413	80.4	334	93.6
	Lecturer	18	3.5	8	2.2
	Other	83	16.1	15	4.2
Total Number of Participants		514		357	

6.3.1 SAUDI PARTICIPANTS

The demographic profile of the Saudi participants in terms of gender, age, highest level of education and occupation in Saudi Arabia is presented in Table 6.10. It is explained that males and females in Saudi Arabia formed 50.6% and 49.4% (1: 0.98), respectively,

of the participants. Due to gender segregation in the Saudi universities, the researcher was able to aim for almost the same ratio of male to female participants, which was obtained by distributing a similar number of questionnaires to both male and female campuses, with the random sampling technique applied within each gender's campus. However, according to Hausman, *et al*, (2010, p.262), although the ratio of males to females in the general population is almost equal (1:1.21), in tertiary education there are more males than females with a ratio of 1: 0.98.

The age distribution within the sample shows that the majority (64.8%) of Saudi participants were aged 18-22. The next major age group was people aged 23-27, which accounted for 22.6% of Saudi participants. The other two age groupings were 28-32 and above 30, with a combined percentage of 12.6% of Saudi participants. The reason for the high percentage of the 18-22 age group is that the majority of university students in both countries are undergraduate students, aged from 18 to 22 years old.

Most of the Saudi participants (80.4%) were students, whereas only 3.5% were lecturers. The rest of the participants (16.1%) were professional technical experts, managers or administrators. In addition 76.7% of Saudi participants were undergraduates, and 16.9% were postgraduates. In addition, 6.8% of Saudi participants claimed that they had gained a PhD.

6.3.2 MALAYSIAN PARTICIPANTS

The demographic profile of Malaysian participants for gender, age, highest level of education and occupation in Malaysia is presented in Table 6.10. It is shows that males form only 24.9% of the Malaysian sample and females 75.1% (a ration of 1: 3.01). This

is due to the fact that at Malaysian universities, a coeducational system is applied and therefore the random sampling has resulted in a sample with a gender ratio that does not reflect the actual gender ratio of the target participants, where there are more females in tertiary education but at a lower ratio of (1.29:1) (Hausman, *et al*, 2010, p.204).

The age distribution among the sample shows that the majority of Malaysian participants (78. 4%) were aged from 18-22. The next major age group was 23-27, which accounted for 14.2% of Malaysian participants. The other two age groups were 28-32 and above 30 with a combined percentage of 7.4% of Malaysian participants. Similarly to Saudi participants, the reason for the high percentage of the 18-22 age group is that the majority of university students in both countries are undergraduate students aged from 18 to 22 year old.

Most Malaysian participants (93.6%) were students, whereas only 2.2% were lecturers. The rest of the participants (4.2%) were professional technical experts, managers or administrators. Moreover, 77.6% of Malaysian participants were undergraduates, whereas 21% were postgraduates. In addition only 1.4% of Malaysian participants claimed that they had gained a PhD.

6.4 INTERNET USAGE

Participants were asked in the questionnaire to provide information about their Internet usage, including information on the number of hours spent on the Internet per week, the number of years using the Internet and the places where they have used the Internet. Table 6.11 presents the findings on internet usage by the participants from Saudi Arabia and Malaysia.

6.4.1 SAUDI PARTICIPANTS

Table 6.11 shows that most (88.3%) of the Saudi participants use the Internet for more than 1 hour a week, of which (38.2%) use the internet from 1 and 10 hours while less than 9% use the Internet for more than 40 hours a week. Most (94.2%) of the Saudi participants have at least one year's experience of using the Internet with more than half (52.5%) have between four and nine years Internet experience. Almost 7% have more than 12 years Internet experience. The majority (96.4%) of the Saudi participants access the Internet at home while less than one-fifth (19%) access the Internet at an Internet café. Only 7.8% access the Internet at the library. In addition, more than a third (38.55) access the Internet via a mobile phone.

6.4.2 MALAYSIAN PARTICIPANTS

Table 6.11 shows that the majority (98.9%) of the Malaysian participants use the Internet for more than 1 hour a week, of which 30.3% use the internet from 1 and 10 hours while almost a fifth (19 %) use the Internet for more than 40 hours a week. The majority (98%) of the Malaysian participants have at least one year's experience of using the Internet while more than half (54.3%) have experienced the Internet for between four and nine years. More than 10.4% had in excess of 12 years Internet experience. The majority (84.7%) of the Malaysian participants access the Internet at home. 61.3% of the participants access the Internet at the library while 60.4% access the Internet in an Internet café. Similarly, to the Saudis more than a third (33.6%) of the Malaysian participants access the Internet via a mobile phone.

Table 6-11: Internet Usage of the participants from Saudi Arabia and Malaysia

		Saudi Arabia		Malaysia	
Internet Usage		**Frequency**	**%**	**Frequency**	**%**
Online hours per week	Less than1 Hour	60	11.7	4	1.1
	1-10 Hours	196	38.2	108	30.3
	11-20 Hours	101	19.6	80	22.4
	21-30 Hours	72	14	61	17.1
	31-40 Hours	39	7.6	36	10.1
	More than 40 Hours	46	8.9	68	19.0
Experience of Internet Usage	Less than1 Year	30	5.8	7	2
	1-3 Years	120	23.3	65	18.2
	4-6 Years	160	31.1	110	30.8
	7-9 Years	110	21.4	84	23.5
	10-12 Years	59	11.5	37	10.4
	More than 12 Years	35	6.9	54	15.1
Access to Internet at Home	Yes	456	96.4	282	84.7
	No	17	3.6	51	15.3
Access to Internet at Internet Café	Yes	90	19	201	60.4
	No	383	81	132	39.6
Access to Internet at Library	Yes	35	7.4	204	61.3
	No	438	92.6	129	38.7
Access to Internet at Work	Yes	94	19.9	59	17.7
	No	379	80.1	274	82.3
Access to Internet from Mobile Phone	Yes	182	38.5	112	33.6
	No	291	61.5	221	66.4
Total Number of Participants		514		357	

6.5 INTERNET ACTIVITIES

In the fifth group of questions in the questionnaire, participants were asked to provide information about the level of their Internet usage for 11 specific Internet activities. With regard to their level of Internet usage, the participants were asked to rate the following items. E-mails, search engines, social network websites, newspaper websites, instant messaging services websites (i.e. using Microsoft Messenger or Skype), online games websites, video sharing websites (i.e. YouTube), live TV and radio websites, e-commerce websites (i.e. to purchase goods or services), online banking websites and e-government websites. In addition, the participants were provided with a scale of five possible levels of usage: never, once or seldom, once or twice a month, at least once a week or almost every day.

The details of the internet activities of the participants from Saudi Arabia and Malaysia are summarised in Appendix E (table 6.16). The level of the usage of the 11 different Internet activities by the Saudi and Malaysian participants were compared using the five possible levels of usage outlined above. In addition, Table 6.17 (see Appendix E) shows further details of the Internet activities of the participants from Saudi Arabia and Malaysia particularly with regard to comparing the percentage of each Internet activity that has been used at least once by participants from both countries.

6.5.1 SAUDI PARTICIPANTS

It appears that more than two-thirds of the Saudi participants (77.9%) use search engine websites almost every day while half used online communication websites including e-mail (57.3%) and instant messaging (54.3%) almost every day. It shows that daily visits to entertainment websites were made by a small number of participants, for example, online games (11.7%) and live TV (6.2%) websites with more participants browsing video sharing websites (33.8%). Table 6.3 also shows that few participants visited business websites on a daily basis, for example, e-commerce (3.1%), online banking (5.8%) and e-government websites (4.3%) (Appendix E - Table 6.16).

Table 6.17 (Appendix E) shows that almost all the respondents in this study (98.8%) had used search engine websites at least once and almost similarly large majorities had used online communication websites including e-mail (96.6%) and instant messaging (90.7%) at least once. It also shows that several types of entertainment websites had been visited at least once by the majority of the Saudi participants, for example, online games (67.8%), video sharing websites (93.6%) and live TV (66.2%) websites. Table

6.4 also shows that more than half of Saudi participants visited business websites at least once, for example, e-commerce (59.2%), online banking (68.7%) and e-government websites (60.2%).

6.5.2 MALAYSIAN PARTICIPANTS

Similar to Saudi participants, more than two thirds of Malaysian participants (70%) use search engine websites almost every day while more than half used online communication websites including e-mail (65%) and instant messaging (51.2%) almost every day. Table 6.17 shows that daily visits to entertainment websites were made by fewer participants, for example, online games (6.3%) and live TV (11%), with more participants browsing video sharing websites (20.7%). It also shows that few participants visited business websites on a daily basis, for example, e-commerce (4.1%), online banking (3.9%) and e-government websites (9.1%) (Appendix E- Table 6.16).

Table 6.17 (Appendix E) shows that similarly to Saudi Arabia almost all the respondents from Malaysia (98.3%) had used search engine websites at least once and a similarly high proportion had used online communication websites including e-mail (99.4%) and instant messaging (96.4%). This shows that entertainment websites have been visited at least once by the majority of both Saudi and Malaysian participants, for example, online game sites (69.1%), video sharing websites (90.9%) and live TV (81.5%) websites. Table 6.4 also shows that more than half of the Malaysian participants had visited business websites at least once, for example, e-commerce (62.31%), online banking (54.3%) and e-government websites (80.7%).

6.6 PRIVACY PERSPECTIVE FACTORS (INDEPENDENT VARIABLES)

Chapter 5 included a discussion of privacy perspective factors, that is, the independent variables in this research. These factors include participants' concerns about submitting personal information and their trust in the way their personal information is handled in 11 different online activities including: e-mails, search engines, social network websites, newspaper, instant messaging services, online games, video sharing, live TV and radio, e-commerce, online banking and e-Government websites. In this section, there are four subsections: firstly privacy concerns, secondly concerns about the misuse of submitted personal information, thirdly privacy trust, including information security and fourthly professional handling of personal information.

6.6.1 PRIVACY CONCERNS

The level of concern among the Saudi and Malaysian participants with regard to submitting personal information via 11 different Internet activities is illustrated in (Appendix E - Table 6.18).

6.6.1.1 Saudi participants

Around a third or more of the Saudi participants expressed concerns about submitting their personal information via search engines (39.8%), newspaper sites (33.2%), communications (e-mail, 39.8%), instant messaging, (44.7%), social networks, (33.6%) and entertainment websites (online games, 31.8%, video sharing websites, 31.1% and live TV 30.7%). Around half or more of the Saudi participants were concerned about

submitting their personal information via business websites (e-commerce, 48.9%, online banking, 52.8% and e-government, 57.7%) (Appendix E - Table 6.18).

6.6.1.2 Malaysian participants

Around half of the Malaysian participants conveyed that they were concerned about submitting their personal information via search engines (50.1%) and newspaper sites (46.3%), while more than two thirds were concerned over communication websites (e-mail, 80%, instant messaging, 68%, and social networks, 67.8%). By contrast, around a third of the Malaysian participants were concerned when they submit their personal information via entertainment websites (online games, 33.3%, video sharing websites, 41.9% and live TV 43.5%). Around half to well over half of the Malaysian participants were concerned about submitting their personal information via business websites (e-commerce, 46%, online banking, 52.6% and e-government, 59.8%) (Appendix E - Table 6.18).

6.6.2 CONCERNS ABOUT THE POSSIBLE MISUSE OF THE SUBMITTED PERSONAL INFORMATION

The level of concern among the Saudi and Malaysian participants about the possible misuse of the submitted personal information, that is, possible unexpected, unauthorised or improper secondary use of the submitted personal information is shown in Appendix E (Table 6.19).

6.6.2.1 Saudi participants

More than two-thirds of the Saudi participants believed that their personal information could be found or used by others, used in an unexpected way or in a manner with which they were not comfortable, threaten their security or invade their privacy, create unexpected problems or be misused in general. Less than a fifth of the participants, however, were unconcerned about the misuse of their personal information (Appendix E- Table 6.19).

6.6.2.2 Malaysian participants

More than three-quarters of the Malaysian participants believed that their personal information could be found or used by others, used in an unexpected way or in a manner with which they were not comfortable, threaten their security or invade their privacy, create unexpected problems or be misused in general. Less than a tenth of the participants, however, were unconcerned about the opportunistic use of their personal information (Appendix E - Table 6.19).

6.6.3 PRIVACY TRUST – INFORMATION SECURITY

The level of trust of the Saudi and Malaysian participants with regard to the safe exchange of their personal information via six different Internet activities is described in Appendix E (Table 6.20).

6.6.3.1 Saudi participants

More than half (51.7%) of the Saudi participants considered e-mail, a safe environment for exchanging their personal information while slightly more than a fifth of believed that social networks (22.1%) and newspaper sites (22.3%) are safe. More than a third trusted instant messaging (37.9%) as a safe environment for the exchange of their personal information. Finally, only a few Saudi participants considered online games (13.2%) and video sharing (10.1%) a safe environment (Appendix E - Table 6.20).

6.6.3.2 Malaysian participants

More than two-thirds (66.9%) of the Malaysian participants considered e-mail a safe environment for the exchange of their personal information while only a third of them believed that social networks are safe (33.1%). More than a quarter considered newspaper sites (27.8%) to be safe while more than a third of the participants trusted instant messaging (44.4%) as a secure environment for the exchange of their personal information. Finally, only a few Malaysian participants considered online games (10.7%) and video sharing (12.9%) to be safe (Appendix E - Table 6.20).

6.6.4 PRIVACY TRUST – PROFESSIONAL HANDLING

The levels of trust among Saudi and Malaysian participants, with regard to the professional handling of their personal information via 11 different websites are illustrated in Appendix E (Table 6.21).

6.6.4.1 Saudi participants

More than two-thirds of Saudi participants express their trust in the professional handling of their personal information via online banking (62.9%) and e-government (63.5%) websites. More than half of the participants (52.6%) trusted e-mail to handle their personal information safely. The table also shows that more than a third of the Saudi participants believed that e-Commerce (41.4%) and instant messaging (34%) can be trusted to handle their personal information while more than a quarter of them share the same belief regarding search engines (31.7%), newspaper sites (29.7%), social networks (27.2%) and live TV (22.3%) websites. In addition, the table illustrates that Saudi participants believed that online games (15.3%) and video sharing (17.7%) websites could be trusted with their personal information (Appendix E - Table 6.21).

6.6.4.2 Malaysian participants

More than three-quarters of the Malaysian participants conveyed their trust in the professional handling of their personal information via e-mail (74.7%). More than half the participants trusted online banking (52.1%) and e-government (61.4%) websites to handle their personal information. The table also shows that more than a third of the Malaysian participants believed that e-Commerce (37.7%), instant messaging (42.1%), newspaper sites (36.9%) and social network (37.2%) websites can be trusted to handle their personal information but only approximately a quarter share the same belief regarding search engines (30.3%) and live TV (23.1%) websites. In addition to this, the table illustrates that Malaysian participants believed that online games (12.1%) and video sharing (14.6%) websites can be trusted with their personal information (Appendix E - Table 6.21).

6.7 THE IMPACTS OF CULTURAL BACKGROUND ON PRIVACY PERSPECTIVES (DEPENDENT VARIABLES)

In the previous chapter, cultural influences on privacy perspectives were proposed as independent variables in this research. They include the effect of religious beliefs, IT skills, social norms (family and friends) and Internet regulation on online privacy attitudes with regard to guarding personal information, care about online privacy, care about others' online privacy and being careful when revealing personal information.

6.7.1 THE IMPACT OF CULTURAL BACKGROUND ON GUARDING PERSONAL INFORMATION

The impact of social norms (family and friends), religious beliefs, internet regulation and IT skills on online privacy attitudes towards guarding personal information is summarised in Appendix E (Table 6.22).

6.7.1.1 Saudi participants

More than two-thirds of the Saudi participants believed that their religion (70.5%), family and friends (66.4%) affect their attitude towards guarding personal information. More than half (55.9%) shared the same belief with regard to the effect of their IT skills on their attitude towards guarding personal information. In addition, almost half of the participants think Internet regulation (49.7%) affected their decisions about guarding personal information (Appendix E- Table 6.22).

6.7.1.2 Malaysian participants

The majority (90.1%) of the Malaysian participants believed that their family and friends affect their attitude towards guarding personal information whereas more than two-thirds (70.8%) shared the same belief with regard to the effect of religion. In addition, more than half of the participants think IT skills (63.6%) and Internet regulation (59.8%) have an effect on their decisions about guarding personal information (Appendix E - Table 6.22).

6.7.2 CARE ABOUT ONE'S PRIVACY

The impact of social norms (family and friends), religious beliefs, internet regulation and IT skills on the attitude towards caring about personal privacy online among Saudi and Malaysian participants is shown Appendix E (Table 6.23).

6.7.2.1 Saudi participants

Almost three-quarters of the Saudi participants believed that their religion (74.8%) affects their attitude towards caring about their online personal privacy whereas more than two-thirds think that family and friends (67%) also affect their attitude towards caring about their personal privacy. More than half of the participants shared the same belief with regard to the effect of IT skills (59.8%) and of internet regulation (56.1%) on their attitude towards caring about their personal privacy (Appendix E - Table 6.23).

6.7.2.2 Malaysian participants

The majority (89%) of the Malaysian participants believed that their family and friends affect their attitude towards caring about their personal privacy whereas more than two-thirds (73.6%) shared the same belief with regard to the effect of religion. Almost two-thirds of the participants think that IT skills (65%) and Internet regulation (61.2%) affect their decisions with regard to caring about their personal privacy (Appendix E - Table 6.23).

6.7.3 CARE ABOUT OTHERS' PRIVACY

The impact of social norms (family and friends), religious beliefs, Internet regulation and IT skills on the attitude of caring about others' privacy online among the Saudi and Malaysian participants is shown in Appendix E (Table 6.24).

6.7.3.1 Saudi participants

More than two thirds of the Saudi participants believed that their religion (70.7%) , family and friends (68.9%) affect their attitude towards caring about others' personal privacy whereas more than half of them think that IT skills (58.3%) and Internet regulation (59.6%) also affect this attitude (Appendix E - Table 6.24).

6.7.3.2 Malaysian participants

The majority of the Malaysian participants believed that their family and friends (89%) and their religion (80.2%) affect their attitude towards caring about others' personal

privacy whereas more than two-thirds shared the same belief regarding the effect of IT skills (64.7%) and Internet regulation (67.8%) Appendix E - Table 6.24).

6.7.4 TAKING CARE WHEN REVEALING PERSONAL INFORMATION

The impact of social norms (family and friends), religious beliefs, Internet regulation and IT skills on the online privacy attitude towards taking care when revealing personal information online among the Saudi and Malaysian participants is shown in Appendix E (Table 6.25).

6.7.4.1 Saudi participants

More than two-thirds of the Saudi participants believed that their religion (70.7%) affects their attitude towards being careful when revealing personal information online whereas more than half of them think that family and friends (59.8%), IT skills (54.2%) and Internet regulation (54.2%) also affect their attitude towards being careful when revealing personal information online (Appendix E - Table 6.25).

6.7.4.2 Malaysian participants

The majority (86.2%) of the Malaysian participants believe that their family and friends affect their attitude towards being careful when revealing personal information online whereas almost three quarters (74.7%) shared the same belief with regard to the effect of religion. In addition, about two-thirds of the participants think IT skills (64.7%) and Internet regulation (65.6%) have an effect on their decisions with regard to taking care when revealing personal information online (Appendix E - Table 6.25).

6.8 CONCLUSION

The aim of this chapter was to summarise the results of the descriptive data analysis for the data collected from Saudi Arabia and Malaysia. The chapter outlined the analysis of the demographic characteristics, Internet usage and activities of both the Saudi and Malaysian participants. It also described the level of participants' online privacy concerns and online trust. The effects of family and friends, religious beliefs, Internet regulation and IT skills on the participants' online privacy attitudes were discussed. This chapter also illustrated the results of the data screening assessments with regard to outliers and normality. The chapter outlined the results of factor analysis and validity (KMO) and reliability (Cronbach's Alpha) tests for both Saudi and Malaysian samples.

7 CHAPTER 7: INFERENTIAL DATA ANALYSIS

7.1 INTRODUCTION

In the previous chapter, the descriptive data analysis for the collected data from both Saudi Arabia and Malaysia was reported together with an analysis of the demographic characteristics of the participants from the two countries, their Internet usage and activities. We also examined the level of online privacy concerns, trust and described the effect of family and friends, religious beliefs, Internet regulation and IT skills on online privacy attitudes. Chapter 6 also provided a data screening assessment with regard to outliers and normality in order to examine the possibility of satisfying the regression assumption that will take place in this chapter as a part of the inferential data analysis. Finally, the chapter assessed the reliability and validity required of the questionnaire before any further data analysis could be undertaken.

This chapter aims to illustrate the advanced phase of the data analysis for the collected data from both Saudi Arabia and Malaysia. This is to answer the research questions of this study, identify the cultural influences that affect the privacy perspectives of individual Saudi and Malaysian Muslims regarding their internet usage and in addition, identify any similarities and differences between these perspectives. The chapter will start with testing the proposed research hypotheses using simple linear regression analysis. This is followed by testing the effect of nationality, gender, age factors on online privacy concerns, trust and the online privacy attitude by using t-tests and ANOVA. Finally, a further analysis of the effects of nationality, gender on online privacy concerns, trust and the online privacy attitude will be done using both contingency tables and chi-square tests of independence.

7.2 REGRESSION FOR TESTING THE RESEARCH HYPOTHESES

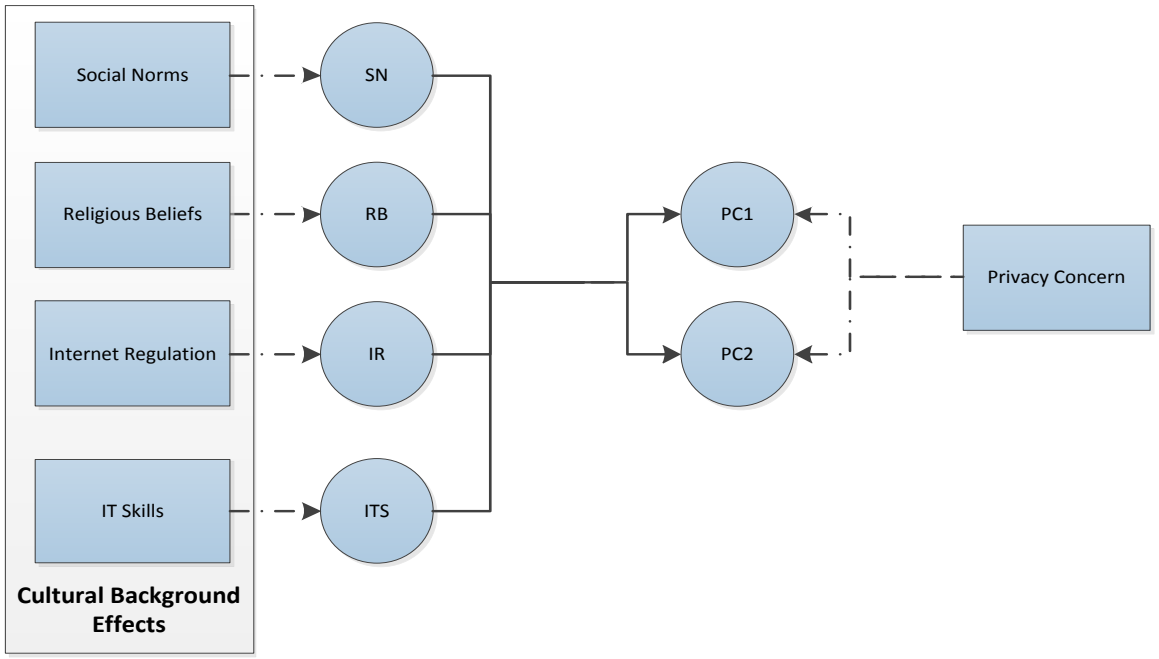
The aim of this section is to test the hypotheses discussed in Chapter 5 and, therefore, to assesses their validity in both the Saudi and Malaysian cases. In order to test these hypotheses, a series of simple linear regression analyses were conducted to calculate Pearson Correlation Coefficients (r), Independent Samples T-tests (t) and P-values (p) on both the Saudi and Malaysian samples. This section is divided into three sub-sections. In the first two sub-sections, the relationship between the individual's religious beliefs, IT skills, social norms and local Internet regulation and their level of both privacy concerns and online trust was assessed by testing hypotheses 1 to 16 for Saudi and Malaysian participants respectively. In the third sub-section, a comparison between Saudi and Malaysian participants was conducted to identify similarities and differences between those factors that affect their privacy concerns and online trust. This is done by testing hypotheses 17 to 20 on both Saudi and Malaysian participants.

As mentioned in 5.4: Research hypotheses), these hypotheses are directional (one-tailed) hypotheses,. They examine the possibility of whether the increase in the privacy concerns (PC-1 and PC-2) and in the Internet trusts (IT-1 and IT-2) are a consequence of the increase in the cultural effects of social norms (SN), religion beliefs (RB), Internet regulation (IR) and IT skills (ITS). However the possibility of the decrease of the privacy concerns (PC-1 and PC-2) and in the Internet trusts (IT-1 and IT-2 as a result of the increase in the cultural effects of social norms (SN), religion beliefs (RB), Internet regulation (IR) and IT skills (ITS) are not examined by these one-tailed hypotheses.

As illustrated in Chapter 5, hypotheses 1 to 4 were designed to answer the first research question. Is there a relationship between the level of an individual's Internet privacy concerns, the effects of their religious beliefs, IT skills, social norms and local Internet regulation on their online privacy attitudes? Hypotheses 5 to 8 were designed to answer the second research question. Is there a relationship between the level of an individual's Internet trust and the effects of their religious beliefs, IT skills, social norms and local Internet regulation on their online privacy attitudes? Hypotheses 9 to 16 were designed to answer the third research question. How well do the impacts of their religious beliefs, IT skills, social norms and local Internet regulation predict their Internet privacy concerns and their Internet trust? Finally, hypotheses 17 to 20 were designed to answer the fourth research question. What are the similarities and differences between individual Muslims from different cultural backgrounds with regard to the impacts of their religious beliefs, IT skills, social norms and local Internet regulation on both their Internet privacy concerns and their Internet trust? In addition, based upon the outcome of factor analysis (Chapter 5), privacy concerns and online trust variables were divided into two further variables. This meant the privacy concerns variable became:

1) An individual's concerns about submitting personal information via the Internet

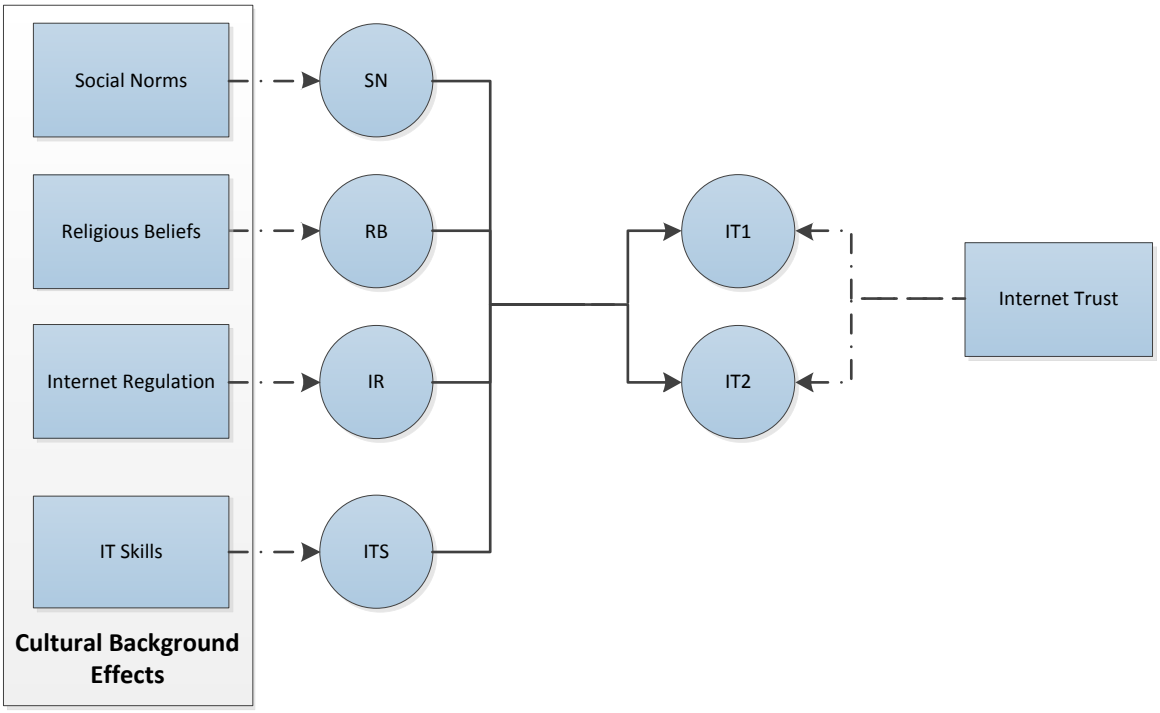
2) An individual's concerns about the unauthorized use of the personal information submitted



Similarly, the online trust variable became:

1) An individual's trust with regard to the professional handling of their personal information via the Internet

2) An individual's trust in the safety of the exchange of their personal information via the Internet



Therefore, each hypothesis from 1 to 16 is divided into two parts (**a)** and (**b)** (see Table 7.1). For example, hypothesis 1, which is **H1:** *A higher level of Internet privacy concerns is related to the greater impact of an individual's religious beliefs on their online privacy attitude*, becomes two hypotheses:

a), *A higher level of concern about submitting personal information via the Internet is related to the greater impact of an individual's religious beliefs on their online privacy attitudes* and

b) *A higher level of concern about unauthorized use of the submitted personal information is related to the greater impact of an individual's religious beliefs on their online privacy attitudes.*

Table 7-1: Hypotheses 1 to 8 and their part of the privacy concern and Internet Trust

Hypotheses	Codes	Description
H1: A higher level of Internet privacy concerns (PC-1 and PC_2) is related to the greater impact of an individual's religious beliefs (RB) on their online privacy attitudes.	H1a	PC_1 ← RB
	H1b	PC_2 ← RB
H2: A higher level of Internet privacy concerns (PC-1 and PC_2) is related to the greater impact of an individual's social norms (SN) on their online privacy attitudes.	H2a	PC_1 ← SN
	H2b	PC_2 ← SN
H3: A higher level of Internet privacy concerns (PC-1 and PC_2) is related to the greater impact of the local Internet regulation (IR) on their online privacy attitudes.	H3a	PC_1 ← IR
	H3b	PC_2 ← IR
H4: A higher level of Internet privacy concerns (PC-1 and PC_2) is related to the greater impact of an individual's IT skills (ITS) on their online privacy attitudes.	H4a	PC_1 ← ITS
	H4b	PC_2 ← ITS
H5: A higher level of Internet Trust (IT-1 and IT_2) is related to the greater impact of an individual's religious beliefs (RB) on their online privacy attitudes.	H5a	IT_1 ← RB
	H5b	IT _2 ← RB
H6: A higher level of Internet Trust (IT-1 and IT_2) is related to the greater impact of an individual's social norms (SN) on their online privacy attitudes.	H6a	IT _1 ← SN
	H6b	IT _2 ← SN
H7: A higher level of Internet Trust (IT-1 and IT_2) is related to the greater impact of the local Internet regulation (IR) on their online privacy attitudes.	H7a	IT _1 ← IR
	H7b	IT _2 ← IR
H8: A higher level of Internet Trust (IT-1 and IT_2) is related to the greater impact of an individual's IT skills (ITS) on their online privacy attitudes.	H8a	IT _1 ← ITS
	H8b	IT _2 ← ITS
H9: The effect Internet users' religious beliefs (RB)on their Internet privacy concerns (PC-1 and PC_2) is greater than that of other factors	H9a	PC_1← RB > SN, IR, ITS
	H9b	PC_2← RB > SN, IR, ITS
H10: The effect of Internet users' social norms (SN) on their Internet privacy concerns (PC-1 and PC_2) is greater than that of other factors	H10a	PC_1← SN > RB, IR, ITS
	H10b	PC_2← SN > RB, IR, ITS
H11: The effect of the Internet regulation in force (IR) in an Internet user's country on their Internet privacy concerns (PC-1 and PC_2) is greater than that of other factors	H11a	PC_1 ← IR> SN, RB, ITS
	H11b	PC_2 ← IR> SN, RB, ITS
H12: The effect of Internet users' IT skills (ITS) on their Internet privacy concerns (PC-1 and PC_2) is greater than that of other factors	H12a	PC ← ITS> SN, RB, IR
	H12b	PC_2 ← ITS> SN, RB, IR
H13: The effect of Internet users' religious beliefs (RB) on their Internet trust (IT-1 and IT_2) is greater than that of other factors	H13a	IT _1← RB > SN, IR, ITS
	H13b	IT_2← RB > SN, IR, ITS
H14: The effect of the social norms (SN) of Internet users on their Internet trust (IT-1 and IT_2) is greater than that of other factors	H14a	IT_1 ← SN > RB, IR, ITS
	H14b	IT_2← SN > RB, IR, ITS
H15: The effect of the Internet regulation in force (IR) in an Internet user's country on their Internet trust (IT-1 and IT_2) is greater than that of the other factors	H15a	IT_1← IR> SN, RB, ITS
	H15b	IT_2← IR> SN, RB, ITS
H16: The effect of Internet users' IT skills (ITS)on their Internet trust (IT-1 and IT_2) is greater than that of other factors	H16a	IT_1 ← ITS> SN, RB, IR
	H16b	IT_2← ITS> SN, RB, IR

7.2.1 SAUDI ARABIA

In this section, three of the research questions, which are covered by the first 16 hypothesises with regard to the Saudi sample, were answered. As explained in chapter five (section 5.4) and in the introduction to this section (7.1), privacy concern and Internet trust were each divided into two parts. The privacy concerns divided:

a) The concern about submitting personal information online and

b) The concern about unauthorized use of the submitted personal information.

Internet trust was divided:

a) The trust of the professional handling of the individual's personal information via the Internet and

b) The trust about the safe exchange of the individual's personal information via the Internet

As table 7.1 shows each of 16 hypotheses, which were derived from the first, second and third research questions were each divided into two parts a and b.

7.2.1.1 First Research Question

The first research question is that is there a relationship between the level of an individual's Internet privacy concerns and the effects of their religious beliefs, IT skills, social norms and local Internet regulation on their online privacy attitudes. This question was answered using hypotheses (H1-H4), which include a) the concern about submitting personal information online and b) the concern about unauthorized use of the submitted personal information:

Hypothesis H1:

A higher level of Internet privacy concerns is related to the greater impact of an individual's religious beliefs on their online privacy attitudes.

The regression test shows that the first part of hypothesis 1, that is, 1**a**) a higher level of concern about submitting personal information via the Internet is related to the greater impact of an individual's religious beliefs on their online privacy attitudes was supported (r = 0.129, r square = 0.015 and p = 0.003). It also shows that the second part of hypothesis 1, that is 1**b)** a higher level of concern about unauthorized use of the submitted personal information is related to the greater impact of an individual's religious beliefs on their online privacy attitudes was also supported (r = 0.188, r square = 0.033 and p < 0.000), (Table 7.2). Therefore, Saudi participants' privacy concerns both with regard to submitting their personal information via the Internet and the possible misuse of the information may be affected by their religious beliefs.

Hypothesis H2:

A higher level of Internet privacy concerns is related to the greater impact of an individual's social norms on their online privacy attitudes.

With regards to the first part of the hypothesis 2**a)** a higher level of concern about submitting personal information via the Internet is related to the greater impact of social norms on the individual's online privacy attitudes was supported according to the regression test (r = 0.104, r square = 0.009 and p < 0.019). The second part of the hypothesis 2**b)** a higher level of concern about inopportune use of the submitted personal information was related to the greater impact of social norms on the individual's online privacy attitudes is supported (r = 0.117 , r square = 0.012 and p <

0.008) (Table 7.2). Therefore, Saudi participants' privacy concerns with regard to submitting personal information via the Internet and the possible misuse of the information may be affected by their social norms.

Hypothesis H3:

A higher level of Internet privacy concerns is related to the greater impact of the local Internet regulation on their online privacy attitudes.

Moving to the first part of the third hypothesis 3**a)** a higher level of concern about submitting personal information via the Internet is related the greater impact of the local Internet regulation on the individual's online privacy attitudes, regression analysis shows that the hypothesis is supported ($r = 0.132$, r square = 0.016 and $p < 0.003$) (Table 7.2). The second part of the third hypothesis **3b)** a higher level of concern about unauthorized use of the submitted personal information is related to the greater impact of Internet regulations on the individual's online privacy attitudes was not supported. This means that the Saudi participants' privacy concerns regarding the submission of personal information via the Internet may be affected by Internet regulation in Saudi Arabia. Their concerns, however, about the possibility of misuse of the submitted personal information are not significantly associated with the impacts of Internet regulation in Saudi Arabia.

Hypothesis H4:

A higher level of Internet privacy concerns is related to the greater impact of the individual's IT skills on their online privacy attitudes.

Regression analysis results supported both parts of the fourth hypothesis. 4**a)** a higher level of concern about submitting personal information via the Internet is related to the

greater impact of the individual's IT skills on their online privacy attitudes (r = 0.143, r square = 0.019 and p < 0.001). **4b)** a higher level of concerns about unauthorized use of the submitted personal information is related to the greater impact of the individual's IT skills on their online privacy attitudes (r = 0.118 , r square = 0.012 and p < 0.007) (Table 7.2). Therefore, the Saudi participants' privacy concerns about submitting personal information via the Internet and the possibility of misuse of the submitted personal information are affected by their IT skills.

7.2.1.2 The Second Research Question

The second research question is that is there a relationship between the level of an individual's Internet trust and the effects of their religious beliefs, IT skills, social norms and local Internet regulation on their online privacy attitudes. This question is answered using the four hypotheses (H5-H8) which include:

a) Trust with regards to the professional handling of the individual's personal information via the Internet and

b) Trust with regard to the safety of the exchange of the individual's personal information via the Internet

Hypothesis H5:

A higher level of Internet trust is related to the greater impact of an individual's religious beliefs on their online privacy attitudes.

With regard to the first part of the fifth hypothesis **5a)** a higher level of trust with regards to the professional handling of the individual's personal information via the Internet is related to the greater impact of religious beliefs on their online privacy attitudes was supported (r = 0.112, r square = 0.011 and p < 0.011) (Table 7.2). The

second part **5b)** a higher level of trust with regard to the safety of the exchange of the individual's personal information via the Internet is related to the greater impact of religious beliefs on their online privacy attitudes was not supported. Therefore, the Saudi participants' trust in the professional handling of their personal information via the Internet is affected by their religious beliefs.

Hypothesis H6:

A higher level of Internet trust is related to the greater impact of an individual's social norms on their online privacy attitudes.

The first part of the sixth hypothesis **6a)** a higher level of trust with regard to the professional handling of the individual's personal information via the Internet is related to the greater impact of social norms on their online privacy attitudes was not supported. The second part of this hypothesis **6b)** a higher level of trust about the safe exchange of the individual's personal information via the Internet is related to the greater impact of social norms on their online privacy attitudes was supported ($r = 0.088$, r square = 0.006 and $p < 0.047$) (Table 7.2). Therefore, the Saudi participants' trust in the safe exchange of their personal information via the Internet is affected by their social norms.

Hypothesis H7:

A higher level of Internet trust is related to the greater impact of the local Internet regulation on their online privacy attitudes.

With regard to the first part of the seventh hypothesis, both parts **7a**) a higher level of trust with regard to the professional handling of the individual's personal information via the Internet is related to the greater impact of Internet regulation on their online privacy attitudes and **7b)** a higher level of trust with regard to the safe exchange of the

individual's personal information via the Internet is related the greater impact of Internet regulation on their online privacy attitudes were supported. For parts their scores were ($r = 0.151$, r square = 0.021 and $p < 0.001$) and ($r = 0.130$, r square = 0.015 and $p < 0.003$) (Table 7.2) respectfully. Hence, the Saudi participants' online trust for both the professional handling of their personal information via the Internet and the safe exchange of their personal information via the Internet are affected by Internet regulation in Saudi Arabia.

Hypothesis H8:

A higher level of Internet trust is related to the greater impact of the of the individual's IT skills on their online privacy attitudes.

The first part of the eighth hypothesis **8a)** higher level of trust with regard to the professional handling of the individual's personal information via the Internet was related to the greater impact of IT skills on their online privacy attitudes was supported ($r = 0.168$, r square = 0.026 and $p < 0.000$) (Table 7.2). The second part of the eighth hypothesis **8b)** a higher level of trust about the safe exchange of the individual's personal information via the Internet was related to the greater impact of their IT skills on their online privacy attitudes was not supported. Therefore, the Saudi participants' trust in the professional handling of their personal information via the Internet is affected by the Internet regulation in Saudi Arabia. Trust in the safe exchange of their personal information via the Internet is not statistically significant with Internet regulation in Saudi Arabia.

Table 7-2: Results of primary hypothesis test using linear regression for Saudi Arabian participants

	Hypothesis	Coefficient (r)	r-square	P	Supported?
H1a	PC-1 ← RB	0.129	0.015	0.003	Yes
H1b	PC-2 ← RB	0.188	0.033	0.000	Yes
H2a	PC-1 ← SN	0.104	0.009	0.019	Yes
H2b	PC-2 ← SN	0.177	0.012	0.008	Yes
H3a	PC-1 ← IR	0.132	0.016	0.003	Yes
H3b	PC-2 ← IR	*Not supported*			
H4a	PC -1← ITS	0.143	0.019	0.001	Yes
H4b	PC-2 ← ITS	0.118	0.012	0.007	Yes
H5a	IT-1 ← RB	0.112	0.011	0.011	Yes
H5b	IT-2 ← RB	*Not supported*			
H6a	IT -1← SN	*Not supported*			
H6b	IT-2 ← SN	0.088	0.006	0.047	Yes
H7a	IT-1 ← IR	0.151	0.021	0.001	Yes
H7b	IT-2 ← IR	0.130	0.015	0.003	Yes
H8a	IT-1 ← ITS	0.168	0.026	0.000	Yes
H8b	IT-2 ← ITS	*Not supported*			

7.2.1.3 The Third Research Question

The third research question is what is the cultural affect on the individual's perspective with regard the Internet privacy concerns and Internet trust? This question was answered using the following 8 hypotheses (H9-H16):

Hypotheses H9-H12:

H9: *The effect of the Internet users' religious beliefs on their Internet privacy concerns is greater than that of other factors.*

H10: *The effect of the Internet users' social norms on their Internet privacy concerns is greater than that of other factors.*

H11: *The effect of the local Internet regulation on the Internet users' privacy concerns is greater than that of other factors.*

H12: *The effect Internet users' IT skills on their Internet privacy concerns is greater than that of other factors.*

Table (7.1) shows the privacy concerns in each of the above hypotheses (H9-H12) can be divided into parts, namely, the concerns about submitting personal information via the Internet and the concerns about the unauthorized use of the submitted personal information. In addition, the Pearson Correlation Coefficients (r) and r square values of the hypotheses 1-4 (Table 7.2), indicated the following. First that the effect of Internet users' IT skills on their concerns about submitting personal information via the Internet is greater than the other factors, that is, religious beliefs, social norms and Internet regulation. Second the effect of Internet users' religious beliefs on their concerns about the unauthorized use of the submitted personal information is greater than the other factors, that is, IT skills, social norms and Internet regulation. Therefore, only the first part of hypothesis 12 and the second part of hypothesis 9 were supported whereas the rest of the two parts of the hypotheses 9-12 are not (Table 7.3).

Hypotheses H13-H16:

H13: *The effect of the Internet users' religious beliefs on their Internet trust is greater than that of other factors.*

H14: *The effect of the Internet users' social norms on their Internet trust is greater than that of other factors.*

H15: *The effect of the local Internet regulation on the Internet users' trust is greater than that of other factors.*

H16: *The effect the Internet users' IT skills on their Internet trust is greater than that of other factors.*

As seen from table (7.1), Internet trust in each of the above hypotheses (H13-H16) can be divided into two parts, namely, the trust of the professional handling of their personal information via the Internet and the trust of exchange in personal information online. In addition, the Pearson Correlation Coefficients (r) and r square values of hypotheses 5-8 (Table 7.2) indicated the following. First, the effect of Internet users' IT skills on their trust with regard to the professional handling of their personal information via the Internet is greater than the other factors, that is, religious beliefs, social norms and Internet regulation. Second, the effect of Internet users' religious beliefs on their trust about the safe exchange of their personal information via the Internet is greater than the other factors. Therefore, only the first part of hypothesis 16 and the second part of hypothesis 13 were supported whereas the remaining the two parts of hypotheses 12-16 were not supported (Table 7.3).

Table 7-3: Results of secondary hypothesis test using linear regression for Saudi Arabian participants

	Hypothesis	Supported?
H9a	PC-1 ← RB > SN, IR, ITS	No
H9b	PC-2 ← RB > SN, IR, ITS	Yes
H10a	PC-1 ← SN > RB, IR, ITS	No
H10b	PC-2 ← SN > RB, IR, ITS	No
H11a	PC-1 ← IR> SN, RB, ITS	No
H11b	PC-2 ← IR> SN, RB, ITS	No
H12a	PC-1 ← ITS> SN, RB, IR	Yes
H12b	PC-2 ← ITS> SN, RB, IR	No
H13a	IT-1 ← RB > SN, IR, ITS	No
H13b	IT-2← RB > SN, IR, ITS	No
H14a	IT-1 ← SN > RB, IR, ITS	No
H14b	IT-2← SN > RB, IR, ITS	No
H15a	IT-1 ← IR> SN, RB, ITS	No
H15b	IT-2← IR> SN, RB, ITS	Yes
H16a	IT-1 ← ITS> SN, RB, IR	Yes
H16b	IT-2← ITS> SN, RB, IR	No

7.2.2 MALAYSIA

In this section, three of the research questions, which are covered by the first 16 hypothesises about the Malaysian sample, were answered. It is worth to mention, again, that privacy concerns and Internet trust each have two parts. The privacy concerns consists of the concern about submitting personal information online and the concern about unauthorized use of the personal information whereas Internet trust contains trust in the professional handling of the individual's personal information via the Internet and trust about the safe exchange of the individual's personal information via the Internet. For that reason each of the 16 hypotheses, based upon the first, second and third research questions were divided into two parts a and b (see Table 7.1).

7.2.2.1 First Research Question

The first research question was is there a relationship between the level of an individual's Internet privacy concerns and the effects of their religious beliefs, IT skills, social norms and local Internet regulation on their online privacy attitudes. This question was answered using the following four hypotheses (H1-H4), which included a) the concern about submitting personal information online and b) the concern about unauthorized use of the submitted personal information.

Hypothesis H1:

A higher level of Internet privacy concerns is related to the greater impact of an individual's religious beliefs on their online privacy attitudes.

The regression test showed that the first part of the first hypothesis **1a)** a higher level of concerns about submitting personal information via the Internet is related to the greater impact of the individual's religious beliefs on their online privacy attitude was not supported. Likewise, the second part of this hypothesis **1b)** a higher level of concern about the unauthorized use of personal information submitted via the Internet is related to the greater impact of the individual's religious beliefs on their online privacy attitudes was supported according to the regression test ($r = 0.174$, r square = 0.03 and $p < 0.001$) (Table 7.4). Therefore, Malaysian participants' privacy concerns about submitting their personal information via the Internet was affected by their religious beliefs whereas the privacy concerns about submitting possible misuse of the submitted personal information was not affected by their religious beliefs.

Hypothesis H2:

A higher level of Internet privacy concerns is related to the greater impact of an individual's social norms on their online privacy attitudes.

With regard to hypothesis 2, the first part, **2a)** a higher level of concern about submitting personal information via the Internet is related to the greater impact of social norms on the individual's online privacy attitude was supported according to the regression test ($r = 0.169$, r square = 0.029 and $p < 0.001$). **2b)** a higher level of concern about the unauthorized use of the submitted personal information is related to the greater impact of social norms on the individual's online privacy attitudes" was, however, supported ($r = 0.229$, r square = 0.052 and $p < 0.000$) (Table 7.4).

Therefore, the Malaysian participants' privacy concerns about both submitting personal information via the Internet and the possible misuse of the submitted personal information, may be affected by their social norms.

Hypothesis H3:

A higher level of Internet privacy concerns is related to the greater impact of the local Internet regulation on their online privacy attitudes.

The first part of hypothesis 3, **3a)** a higher level of concern about submitting personal information via the Internet is related to greater impact of local Internet regulation on an individual's online privacy attitudes, regression analysis shows that the hypothesis was supported ($r = 0.208$, r square = 0.043 and $p < 0.000$). The second part of this hypothesis **3b)** a higher level of concern about the unauthorized use of submitted personal information is related to the greater impact of local Internet regulation on the individual's online privacy attitude was also supported ($r = 0.232$, r square = 0.054 and $p < 0.000$) (Table 7.4). Thus, Malaysian participants' privacy concerns about submitting

personal information via the Internet may be affected by Internet regulation in Malaysia. Their concerns, however, about the possible misuse of submitted personal information were not significantly associated with the effect of any Internet regulation in Malaysia.

Hypothesis H4:

A higher level of Internet privacy concerns is related to the greater impact of the individual's IT skills on their online privacy attitudes.

Regression analysis results supported both parts of hypothesis 4. **4a)** a higher level of concern about submitting personal information via the Internet is related to the greater impact of the individual's IT skills on their online privacy attitudes ($r = 0.197$, r square $= 0.039$ and $p < 0.000$). **4b)** a higher level of concern about unauthorized use of the submitted personal information is related to the greater impact of the individual's IT skills on their online privacy attitudes ($r = 0.234$, r square $= 0.055$ and $p < 0.000$) (Table 7.4). Therefore, the Malaysian participants' privacy concerns about both submitting personal information via the Internet and the possible misuse of the submitted personal information were affected by their IT skills.

7.2.2.2 The Second Research Question

The second research question was is there a relationship between the level of an individual's Internet trust and the effects of their religious beliefs, IT skills, social norms and local Internet regulation on their online privacy attitudes. This question is answered using the following four hypotheses (H5-H8) which include a) trust about the professional handling of the individual's personal information via the Internet and b) trust with regard to the safety of the exchange of the individual's personal information via the Internet:

Hypothesis H5:

A higher level of Internet trust is related to the greater impact of an individual's religious beliefs on their online privacy attitudes

With regard to hypothesis 5, the first part **5a)** a higher level of trust with regard to the professional handling of one's personal information via the Internet is related to the greater impact of the individual's religious beliefs on their online privacy attitudes was not supported (Table 7.4). The second part **5b)** a higher level of trust in the safe exchange of one's personal information via the Internet is related to the greater impact of the individual's religious beliefs on their online privacy attitudes was also not supported (Table 7.4). Therefore, Malaysian participants' online trusts in both the professional handling of their personal information and in the safe exchange of one's personal information via the Internet were not affected by their religious beliefs.

Hypothesis H6:

A higher level of Internet trust is related to the greater impact of an individual's social norms on their online privacy attitudes.

The first part of the sixth hypothesis **6a)** a higher level of trust with regard to the professional handling of one's personal information via the Internet is related to the greater impact of social norms on the individual's online privacy attitudes was supported ($r = 0.105$, r square = 0.011 and $p < 0.047$). **6b)** a higher level of trust in the safe exchange of one's personal information via the Internet is related to of the greater impact of social norms on the individual's online privacy attitudes" was also supported ($r = 0.123$, r square = 0.015 and $p < 0.020$) (Table 7.4). Therefore, Malaysian participants' trusts in both the professional handling of their personal information via

the Internet and in the safe exchange of their personal information via the Internet were affected by their social norms.

Hypothesis H7:

A higher level of Internet trust is related to the greater impact of the local Internet regulation on their online privacy attitudes.

The first part of the seventh hypothesis **7a)** a higher level of trust with regard to the professional handling of one's personal information via the Internet is related to the greater impact of local Internet regulation on the individual's online privacy attitudes is was supported ($r = 0.116$, r square = 0.014 and $p < 0.02$). The second part **7b)** a higher level of trust in the safety of the exchange of the personal information via the Internet is related to the greater impact of local Internet regulation on the individual's online privacy attitudes was not supported. Hence, Malaysian participants' online trust in the professional handling of their personal information via the Internet was affected by Internet regulation in Malaysia. Malaysian participants' trust in the safe exchange of their personal information via the Internet, however, is not affected by the Internet regulation in Malaysia.

Hypothesis H8:

A higher level of Internet trust is related to the greater impact of the of the individual's IT skills on their online privacy attitudes..

The first part of the eighth hypothesis **8a)** a higher level of trust with regard to the professional handling of one's personal information via the Internet is related to the greater impact of the individual's IT skills on their online privacy attitudes was not supported (Table 7.11). The second part of this hypothesis **8b)** a higher level of trust in

the safe exchange of the one's personal information via the Internet is related to a higher level of the effect of the individual's IT skills on their online privacy attitudes was not supported. Therefore, Malaysian participants' trust in the professional handling of their personal information via the Internet is an effect of Internet regulation in Malaysia. Their trust, however, in the safe exchange of their personal information via the Internet is not statistically associated with Internet regulation in Malaysia (Table 7.4).

Table 7-4: Results of primary hypothesis test using linear regression for Malaysian participants

	Hypothesis	Coefficient	r square	P	Supported?
H1a	*PC-1 ← RB*	*Not supported*			
H1b	*PC-2 ← RB*	0.174	0.03	0.001	Yes
H2a	PC-1 ← SN	0.169	0.029	0.001	Yes
H2b	PC-2 ← SN	0.229	0.052	0.000	Yes
H3a	PC-1 ← IR	0.208	0.043	0.000	Yes
H3b	PC-2 ← IR	0.232	0.054	0.000	Yes
H4a	PC-1 ← ITS	0.197	0.039	0.000	Yes
H4b	*PC-2 ← ITS*	0.234	0.055	0.000	Yes
H5a	IT-1 ← RB	*Not supported*			
H5b	IT-2 ← RB	*Not supported*			
H6a	IT-1 ← SN	0.105	0.011	0.047	Yes
H6b	IT-2 ← SN	0.123	0.015	0.020	Yes
H7a	IT-1 ← IR	0.116	0.014	0.028	Yes
H7b	IT-2 ← IR	*Not supported*			
H8a	IT-1 ← ITS	*Not supported*			
H8b	*IT-2 ← ITS*	*Not supported*			

7.2.2.3 The Third Research Question

Third research question is what is the most cultural affect on the individual perspective with regard the Internet privacy concerns and Internet Trust? This question was answered by using the following 8 hypotheses (H9-H16).

Hypotheses H9-H12:

H9: *The effect of the Internet users' religious beliefs on their Internet privacy concerns is greater than that of other factors*

H10: *The effect of the Internet users' social norms on their Internet privacy concerns is greater than that of other factors*

H11: *The effect of the local Internet regulation on the Internet users' privacy concerns is greater than that of other factors*

H12: *The effect Internet users' IT skills on their Internet privacy concerns is greater than that of other factors*

As seen from table (7.1), the privacy concerns in each of the above hypotheses (H9-H12) can be divided into parts, namely, the concerns about submitting personal information via the Internet and the concerns about the unauthorized use of the submitted personal information. The Pearson Correlation Coefficients (r) and r square values of the hypotheses 1-4 (Table 7.4) indicated the following. First, the effect of social norms on Internet users' concerns about submitting personal information via the Internet is greater than the other factors, that is, religious beliefs, IT skills and Internet regulation. Second, the effect of Internet users' religious beliefs on their concerns about the unauthorized use of submitted personal information is greater than the other factors, that is, IT skills, social norms and Internet regulation. Therefore, only the first part of hypothesis 10 and the second part of hypothesis 9 were supported whereas the remaining two parts of hypotheses 9-12 were not (Table 7.5).

Hypotheses H13 –H16

H13: *The effect of the Internet users' religious beliefs on their Internet trust is greater than the other factors.*

H14: *The effect of the Internet users' social norms on their Internet trust is greater than the other factors.*

H15: *The effect of the local Internet regulation on the Internet users' trust is greater than the other factors.*

H16: *The effect of the Internet users' IT skills on their Internet trust is greater than the other factors.*

As can be seen from table (7.1), the Internet trust in each of the above hypotheses (H13-H16) can be divided into parts, namely, the trust of the professional handling of their personal information via the Internet and the trust of exchange the personal information online. The Pearson Correlation Coefficients (r) and r square values of the hypotheses 5-8 (Table 7.4) indicated that the effect of social norms on both the Internet users' trust in the professional handling of their personal information via the Internet and trust in its exchange online is greater than the other factors, that is, religious beliefs, IT skills and Internet regulation. Therefore, both parts of hypothesis 13 were supported whereas the rest of the two parts of the hypotheses 14-16 were not (Table 7.5).

Table 7-5: Results of secondary hypothesis test using linear regression for Malaysian participants

	Hypothesis	Supported?
H9a	PC-1 ← RB > SN, IR, ITS	No
H9b	PC-2 ← RB > SN, IR, ITS	No
H10a	PC-1 ← SN > RB, IR, ITS	No
H10b	PC-2 ← SN > RB, IR, ITS	No
H11a	PC-1 ← IR> SN, RB, ITS	Yes
H11b	PC-2 ← IR> SN, RB, ITS	No
H12a	PC-1 ← ITS> SN, RB, IR	No
H12b	PC-2 ← ITS> SN, RB, IR	Yes
H13a	IT-1 ← RB > SN, IR, ITS	No
H13b	IT-2← RB > SN, IR, ITS	No
H14a	IT-1 ← SN > RB, IR, ITS	No
H14b	IT-2← SN > RB, IR, ITS	Yes
H15a	IT-1 ← IR> SN, RB, ITS	Yes
H15b	IT-2← IR> SN, RB, ITS	No
H16a	IT-1 ← ITS> SN, RB, IR	No
H16b	IT-2← ITS> SN, RB, IR	No

7.2.3 BOTH SAUDI ARABIA AND MALAYSIA

The fourth research question with regards both Saudi and Malaysian samples, is what are the similarities and differences between individual Muslims from different cultural backgrounds with regard to the effects of their religious beliefs and IT skills.

To answer this research question, four hypotheses (H17-H20) were tested. These hypotheses were tested by a regression analysis between the privacy perspective (PP) in both Saudi and Malaysian samples and the four cultural affects on the online privacy attitude. The privacy perspective (PP) in this test is the sum of the two parts of the privacy concerns (PC-1 and PC-2) and the two parts of Internet trust (IT-1 and IT-2) whereas the four cultural affects on the online privacy attitude are the religious belief (RB), social norms (SN), Internet regulation (IR) and IT skills (ITS).

Hypothesis H17:

The influence of individuals' religious beliefs over their privacy perspective is greater for those in Malaysia than for those in Saudi Arabia

The regression test shows that the coefficient correlation value between privacy perspective (PP) and the affect of the religious believe (RB) in the Malaysian sample is (r = 0.184) whereas in Saudi sample it is (r =0.22). Therefore, this hypothesis was not supported, as the association between the religious belief factor and the Saudi privacy perspective has a higher level for the Pearson Correlation Coefficients than the association between the religious belief factor and the Malaysian privacy perspective (Table. 7.6)**.**

Hypothesis H18:

The influence of social norms on the individual's privacy perspective is greater in Malaysia than in Saudi Arabia

Table 7.6 shows the coefficient correlation values of the regression between the privacy perspective (PP) and the effect of the social norms (SN) in the Malaysian sample is (r = 0.268) and in the Saudi sample is (r =0.159). According to the results of the regression analysis, the hypothesis was supported, as the association between the social norms factor and Malaysian privacy perspective has a higher level of Pearson Correlation Coefficients than the association between the social norms factor and the Saudi privacy perspective.

Hypothesis H19:

The influence of Internet regulations over the individual's privacy perspective is greater in Malaysia than in Saudi Arabia

The regression test shows that the coefficient correlation value between the privacy perspective (PP) and the affect of Internet regulation (IR) in the Malaysian sample is (r = 0.209) whereas in Saudi sample it is (r =0.203). Therefore, according to this result, this hypothesis was not supported. This is because the association between the Internet regulation factor and the Malaysian privacy perspective has a similar Pearson Correlation Coefficient to that for the association between the Internet regulation factor and the Saudi privacy perspective (Table. 7.6)**.**

Hypothesis H20:

The influence of the individual's IT skills over their privacy perspective is greater in Malaysia than in Saudi Arabia

Table 7.6 shows the coefficient correlation values of the regression between the privacy perspective (PP) and the affect of IT skills (ITS) in the Malaysian sample is (r = 0.236) and in the Saudi sample is (r =0.224). Therefore, according to the result of the regression analysis, this hypothesis was not supported as; again, the association between the IT skills factor and Malaysian privacy perspective has almost the same Pearson Correlation Coefficients as that for the association between the IT skills factor and the Saudi privacy perspective (Table. 7.6)**.**

Table 7-6: Results of Further Hypothesis Test using Linear Regression for Both Saudi and Malaysian participants

	Association	Coefficient Correlation		Hypothesis	Supported?
		Malaysian	Saudi		
H17	PP ← RB	0.184	0.225	Malaysian > Saudi Arabia	No
H18	PP ← SN	0.268	0.159	Malaysian > Saudi Arabia	Yes
H19	PP ← IR	0.209	0.203	Malaysian > Saudi Arabia	No
H20	PP ← ITS	0.236	0.224	Malaysian > Saudi Arabia	No

7.2.4 SUMMARY OF THE RESULTS FOR SAUDI ARABIA AND MALAYSIA

Before summarising the relationship between Internet users' privacy perspectives and the four cultural effects on online privacy attitudes, it is worth restating the components of both the privacy perspective and the proposed cultural effect. As mentioned in Chapter 5, the privacy perspective consists of privacy concerns about submitting personal information via the Internet, about the unauthorized use of any personal information that is submitted, trust with regard to the professional handling of one's personal information via the Internet and trust in the safe exchange this information. In addition, the four cultural effects that were examined with regard to online privacy attitudes are religious beliefs, IT skills, social norms and local Internet regulation. There now follows a summary of the relationship between Internet users' privacy perspectives and the four cultural effects on online privacy attitudes according to the regression analysis for both Saudi and Malaysian participants.

Concerning the Malaysian participants, the level of an individual's concerns about submitting personal information via the Internet was related to the impact of their IT skills, social norms and local Internet regulation on their online privacy attitudes; however, social norms tend to be the most influential factor. Moreover, the level of an individual's concerns about the unauthorized use of their personal information is related to the impact of their social norms and local Internet regulation on their online privacy attitudes; however, Internet regulation tends to be the most influential factor. In addition, the level of an individual's trust with regard to the professional handling of personal information via the Internet is related to the impact of their religious beliefs, IT skills, social norms and local Internet regulation on their online privacy attitudes; however, social norms tend to be the most influential factor. Furthermore, the level of an individual's trust in the safe exchange of the personal information via the Internet is related to the impact of their religious beliefs, social norms and Internet regulation on their online privacy attitudes; however, Internet regulation tends to be the most influential factor.

Regarding the Saudi participants, the level of an individual's concerns about submitting personal information via the Internet is related to the impact of their religious beliefs, IT skills, social norms and local Internet regulation on their online privacy attitudes; however, IT skills tend to be the most influential factor. Moreover, the level of an individual's concerns about unauthorized use of personal information that is submitted is related to the level of the effect of their religious beliefs and IT skills on their online privacy attitudes; however, religious beliefs tend to be the most influential factor. In addition, the level of an individual's trust with regard to the professional handling of

their personal information via the Internet is related to the level of their religious beliefs, IT skills and social norms on their online privacy attitudes; however, IT skills tend to be the most influential factor. Furthermore, the level of an individual's trust in the safe exchange of their personal information via the Internet is related to the level of the effect of their religious beliefs, social norms and Internet regulation on their online privacy attitudes; however, religious beliefs tend to be the most influential factor.

Finally, the researcher compared the relationship between the privacy perspective and the impact of the four cultural effects on the online privacy attitudes of Saudi and Malaysian participants using the regression test. The results were as follows. First, religious beliefs tend to have the greatest cultural effect on Saudi privacy perspectives compared to Malaysian privacy perspectives, which are affected more by social norms. Second, the Internet regulations in each country and the IT skills of participants tended to have an equal effect on the privacy perspectives of the participants in both countries. Further discussion on how these results fit with the research model (Figure 5.1) is included in Chapter 8, sections 8.4.1 and 8.4.2.

7.3 T-TEST AND ANOVA TO EXAMINE THE EFFECT OF THE DEMOGRAPHIC FACTORS

The aim of this section is to test the affect of the demographic factors nationality, gender and age of the participants on their privacy concerns and Internet trust, which are the dependent variables of this study. In addition, it aims to test the effect of these demographic factors on the cultural effects i.e. religious beliefs (RB), social norms (SN), Internet regulations (IR) and IT skills (ITS), which are the independent variables

of this study. In order to test the affect of these demographic factors, a series of t-test and ANOVA techniques were used.

The t-test is used to find significant differences between two-level categorical groups, which in this study are nationality (Saudi and Malaysian) and gender (Male and Female). There are two types of t-test. One type is the independent-sample t-test, which is used to compare two different (independent) groups of a given variable. The second type is the paired-sample t-test (also called the dependent t-test), which compares the same group within one variable on two occasions. The dependent and independent variables in both t-tests are the same. The variable that is measured is the dependent variable and the grouping variable is the independent variable. Moreover, the variables could be categorical or continuous. If the variable has values that function as labels rather than numbers then the variable is called categorical and if the variable has numeric values then the variable is continuous. In this research, we have two variables: categorical independent variables as gender (male/ female) or nationality (Saudi/Malaysian) and 8 continuous dependent variables, privacy concerns 1, privacy concerns 2, Internet trust 1, Internet trust 2, religious beliefs, social norms, Internet regulations or IT skills.

In addition, ANOVA analysis is used to find significant differences between three (or more) levels of categorical groups, which are, in this study, the age groups. There are five age groups, in this research, 18-20, 21-23, 24-30, 31-40 and more than 40. In this research the affect of age in the Saudi and Malaysian samples is tested using the ANOVA analysis between the age groups as a categorical independent variable and

eight continuous dependent variables, privacy concerns 1, privacy concerns 2, Internet trust 1, Internet trust 2, religious beliefs, social norms, Internet regulations or IT skills.

Additionally, in order for the t-test and ANOVA to be accurate the researcher needed to ensure sure that the following five assumptions were applied to the samples. First, the scale of measurement should be continuous. Second, the sample is random. Third, each observation is independent of the others. Fourth, the sample should be normally distributed. Fifth, the homogeneity of variance i.e. the variances for two groups should be the same (equal).

With regard to the first assumption i.e. using a continuous variable as the scale of measurement, all the examined variables: privacy concerns, Internet trust, religious beliefs, social norms, Internet regulations and IT skills are measured as continuous values (1-5 in which 1 is strongly disagree and 5 is strongly agree). Regarding the use of random samples, as explained in chapter 5 that the method used in this research is the multi-stage random sampling technique. In addition, each observation (case) in this research originates from random participants and are not affected by others' opinions. With regard to the normal distribution assumptions, as explained in chapter six, both Saudi and Malaysian samples are normally distributed. Finally, the test for the equality of variances would be conducted within the t-test by using Levene's test, which need to be not significant (i.e. greater than 0.05) to be satisfied. The details on the affects of nationality, gender and age group on both independent and dependent variables are explained in the following sub-sections.

7.3.1 THE EFFECT OF NATIONALITY

In this section, the results of the t-test between nationality (Saudi/Malaysian) as a categorical independent variable and the eight continuous dependent variables were reported. The continuous dependent variables were:

- dependent online personal information (PI)
- the Internet user's concerns over submitting personal information online (PC_1)
- the Internet user's concerns over the possible unexpected unauthorised or improper secondary use of the submitted personal information (PC_2)
- the Internet user's concerns over handling personal information online (IT_1)
- the Internet user's trust over the safety of the exchange (IT_2)
- the effect of the religion belief RB, social norms (SN)
- local Internet regulation (IR)
- IT Skills (ITS variables)

A number of t-tests conducted on 757 cases (on both Saudi and Malaysian samples) show that there were differences between Malaysian and Saudi participants in privacy concerns 1, privacy concerns 2, Internet trust 1, Internet trust 2, the affect of social norms, local Internet regulation and IT skills on the online privacy attitude. A further t-test showed also that there was no difference between Malaysian and Saudi participants in the affect of the effect of religious belief on the online privacy attitude (Table 7.7). The following paragraphs and sub-sections describe the details of the t-test results.

With regard to online personal information PI, the independent t-test was conducted to compare the PI scores for Malaysian and Saudi. There was a significant difference in

scores for Malaysian (M = 3.31, SD = 0.43) and Saudi (M = 3.18, SD = 0.39) with t score = 4.43 and p<0.000. The magnitude of the differences in the means (mean difference = 0.13, 95%, CI: 0.07 to 0.19) was very small (eta squared = 0.03).

With regard to the Internet user's concerns over submitting personal information online PC_1, the independent t-test was conducted to compare PC_1 1 scores for Malaysian and Saudi. There was a significant difference in scores for Malaysian (M = 3.36, SD = 0.49) and Saudi (M = 3.05, SD = 0.47) with t score = 8.77 and p<0.000. The magnitude of the differences in the means (mean difference = 0.31, 95%, CI: 0.24 to 0.38) was moderate (eta squared = 0.09).

Moving to the Internet user's concerns over the possible unexpected, unauthorised or improper secondary use of the submitted personal information PC_2, the independent t-test was conducted to compare the PC_2 scores for the Malaysian and Saudi sample populations. There was a significant difference in scores for Malaysian (M = 3.81, SD = 0.32) and Saudi (M = 3.65, SD = 0.59) with t score = 4.83 and p<0.000. The magnitude of the differences in the means (mean difference = 0.16, 95%, CI: 0.95 to 0.23) was very small (eta squared = 0.03).

In addition, both the Internet user's concerns over handling personal information online IT_1 and the Internet user's trust over the safety of the exchange IT_2 were found to be different among Malaysian and Saudi participants. The independent t-test, which were conducted to compare the IT_1 scores for Malaysian and Saudi participants showed a significant difference in scores for Malaysian (M = 3.11, SD = 0.51) and Saudi (M =

3.01, SD = 0.50) with t score = 2.79 and p<0.000. The magnitude of the differences in the means (mean difference = 0.10, 95%, CI: 0.03 to 0.18) was very small (eta squared = 0.01). The independent t-test which, was conducted to compare IT_2 scores for Malaysian and Saudi participants, show that there was a significant difference in scores for Malaysian (M = 2.97, SD = 0.54) and Saudi (M = 2.75 , SD = 0.53) with t score = 5.44 and p<0.000. The magnitude of the differences in the means (mean difference = 0.21, 95%, CI: 0.14 to 0.29) was very small (eta squared = 0.04).

Furthermore, the independent t-tests showed that there were differences between Malaysian and Saudi participants that pertains to the effect of the Social Norms SN, Internet regulation IR and the IT skills ITS on the online privacy attitudes. The t-test results were as follows. First, the scores for the social norms for Malaysian and Saudi participants were a significantly different, for Malaysian (M = 3.90, SD = 0.21) and Saudi (M = 3.58, SD = 0.52) with t score = 11.56 and p<0.000. The magnitude of the differences in the means (mean difference = 0.32, 95%, CI: 0.26 to 0.37) was large (eta squared = 0.15). Second, the Internet regulation scores for Malaysian and Saudi participants were significantly different, for Malaysian (M = 3.61, SD = 0.47) and Saudi (M = 3.45, SD = 0.59) with t score = 4.18 and p<0.000. The magnitude of the differences in the means (mean difference = 0.16, 95%, CI: 0.09 to 0.24) was very small (eta squared = 0.02). Three, the scores for the IT skills for Malaysian and Saudi participants were significantly different, for Malaysian (M = 3.62, SD = 0.48) and Saudi (M = 3.48, SD = 0.57) with t score = 3.76 and p<0.000. The magnitude of the differences in the means (mean difference = 0.14, 95%, CI: 0.07 to 0.22) was very small (eta squared = 0.02).

Table 7-7: The effect of nationality using the t-test on both Saudi and Malaysian participants

Variables	Malaysian		Saudi		*t*	eta	*p*	Different?
	Mean	SD	Mean	SD				
IP	3.31	0.43	3.18	0.39	4.43	0.03	0.00	Small Difference
PC_1	3.36	0.49	3.05	0.47	8.77	0.09	0.00	Moderate Difference
PC_2	3.81	0.32	3.65	0.59	4.83	0.03	0.00	Small Difference
IT_1	3.11	0.51	3.01	0.5	2.79	0.01	0.00	Small Difference
IT_2	2.97	0.54	2.75	0.53	5.44	0.04	0.00	Small Difference
RB	P value is not significant, so there are no difference							
SN	3.90	0.21	3.58	0.52	11.56	0.15	0.00	Large Difference
IR	3.62	0.47	3.45	0.59	4.18	0.02	0.00	Small Difference
ITS	3.62	0.48	3.48	0.57	3.76	0.02	0.00	Small Difference

7.3.2 THE EFFECT OF GENDER

In this section, the results of the t-test between gender as a categorical independent variable and eight continuous dependent variables as described below. The continuous dependent variables were:

- online personal information (PI)
- the Internet user's concerns over submitting personal information online (PC_1)
- the Internet user's concerns over the possible unexpected, unauthorised or improper secondary use of the submitted personal information (PC_2)
- the Internet user's concerns over handling personal information online (IT_1)
- the Internet user's trust over the safety of the exchange (IT_2)
- the effect of the religious belief (RB)
- social norms (SN)
- local Internet regulation (IR)
- IT Skills (ITS variables)

Tests were carried out on both Saudi and Malaysian samples.

With regard to the Malaysian sample, t-tests showed that there were no differences between Malaysian male and female participants throughout all the variables. With the Saudi sample, t-tests showed that differences between male and female participants existed with respect to privacy concerns 1, privacy concerns 2, Internet trust 1, Internet trust 2 and the effect of the social norms, local Internet regulation and IT skills on the online privacy attitude. The t-test showed also that there was no difference between male and female participants in the effect of the religious belief on the online privacy attitude (Table 7.8). The details of the t-test results on the Saudi sample are described as follows.

With regard to Saudi Internet user's concerns over the possible unexpected, unauthorised or improper secondary use of the submitted personal information PC_2, the independent t-test was conducted on the PC_2 scores for male and female. There was a significant difference in scores for Male (M = 3.57, SD = 0.65) and Female (M = 3.75, SD = 0.49) with t score = -3.24 and $p<0.000$. The magnitude of the differences in the means (mean difference =- 0.17, 95%, CI: -0.28 to -0.07) was very small (eta squared = 0.02).

Regarding the Saudi Internet user's concerns over handling personal information online IT_1 and the Internet user's trust over the safety of the exchange IT_2, independent t-tests were conducted on the IT_1 and IT_2 scores for Male and Female. The results showed that there was a significant difference in scores for Male (M = 3.06, SD = 0.48) and Female (M = 2.95, SD = 0.50) with t score = 2.46 and $p<0.014$. The magnitude of the differences in the means (mean difference = 0.11, 95%, CI: 0.02 to 0.20) was very

small (eta squared = 0.01) and there was a significant difference in scores for Male (M = 2.83, SD = 0.55) and Female (M = 2.66, SD = 0.50) with t score = 3.36 and p<0.001. The magnitude of the differences in the means (mean difference = 0.17, 95%, CI: 0.07 to 0.26) was very small (eta squared = 0.02).

Finally, the effect of the Religious Believe RB on the online privacy attitude were tested using the independent t-test for Male and Female. In this test the result showed a significant difference in scores for Male (M = 3.64, SD = 0.47) and Female (M = 3.78, SD = 0.39) with t score = -3.40 and p<0.001. The magnitude of the differences in the means (mean difference = -0.14, 95%, CI: -0.22 to -0.06) was very small (eta squared = 0.03).

Table 7-8: The effect of the Gender using the t-test for Saudi participants

Variables	Male		Female		*t*	eta	*p*	Different?
	Mean	SD	Mean	SD				
IP	P value is not significant, so there are no difference							
PC_1								
PC_2	3.57	0.65	3.75	0.49	-3.24	0.02	0.00	Small Difference
IT_1	3.06	0.48	2.95	0.50	2.46	0.01	0.00	Small Difference
IT_2	2.83	0.55	2.66	0.50	3.36	0.02	0.00	Small Difference
RB	3.64	0.47	3.78	0.39	-3.40	0.03	0.00	Small Difference
DN	P value is not significant, so there are no difference							
IR								
ITS								

7.3.3 THE EFFECT OF AGE GROUP

In this section, the results of the ANOVA between the age group as a categorical independent variable and nine continuous dependent variables are described below. The dependent variables were:

- online personal information (PI)

- the Internet user's concerns over submitting personal information online (PC_1)
- the Internet user's concerns over the possible unexpected, unauthorised or improper secondary use of the submitted personal information (PC_2)
- the Internet user's concerns over handling personal information online (IT_1)
- the Internet user's trust over the safety of the exchange (IT_2)
- the effect of the religious belief (RB)
- social norms (SN)
- local Internet regulation (IR)
- IT Skills (ITS variables)

Tests were carried out on both Saudi and Malaysian samples

7.3.3.1 Saudi Arabia

Two variables were found to be affected by the age of the Saudi participants, which were the Internet user's concerns over submitting personal information online and the affect of religious belief on the online privacy attitude. The other variables showed no statistical significance differences. The follow are the details of the test's findings (Table 7.9).

A one-way between-groups analysis of variance was conducted to explore the impact of age on the level of the Internet user's concerns over submitting personal information online (PC_1). Saudi participants were divided into five groups according to their age (18-20, 20-23, 24-30, 31-40 and over 40). There was a statistically significant difference at the $p<0.05$ level in PC_1 scores for the five age groups: $F\ (4, 450) = 6.075$, $p<0.000$.

Despite reaching statistical significance, the actual difference in the mean score between the groups was moderate. The effect size, calculated using eta squared was 0.05.

A one-way between-groups analysis of variance was conducted to explore the impact of age on the level of the affect of religious belief on the online privacy attitude (RB). Saudi participants were divided into five groups according to their age (18-20, 20-23, 24-30, 31-40 and over 40). There was a statistically significant difference at the $p<0.05$ level in RB scores for the five age groups: $F\ (4, 450) = 2.69$, $p<0.000$. Despite reaching statistical significance, the actual difference in the mean score between the groups was small. The effect size, calculated using eta squared was 0.03.

7.3.3.2 Malaysia

Two variables were found to affected by the age of the Malaysian participants, which are the Internet user's concerns over submitting personal information online and the affect of the local Internet regulation on the online privacy attitude. The other variables showed no statistical significance differences. The following are the details of the test's findings (Table 7.10).

A one-way between-groups analysis of variance was conducted to explore the impact of age on the level of the Internet user's concerns over the possible unexpected, unauthorised or improper secondary use of their submitted personal information (PC_2). Saudi participants were divided into five groups according to their age (18-20, 20-23, 24-30, 31-40 and over 40). There was a statistically significant difference at the $p<0.05$ level in PC_2 scores for the five age groups: $F\ (4, 450) = 2.97$, $p<0.000$. Despite reaching statistical significance, the actual difference in the mean score between the groups was small. The effect size, calculated using eta squared was 0.03.

A one-way between-groups analysis of variance was conducted to explore the impact of age on the degree of the effect of local Internet regulation on the online privacy attitude (IR). Saudi participants were divided into five groups according to their age (18-20, 20-23 24-30, 31-40 and over 40). There was a statistically significant difference at the $p<0.05$ level in IR scores for the five age groups: $F\ (4, 450)$ = 3.38, p<0.000. Despite reaching statistical significance, the actual difference in the mean score between the groups was moderate. The effect size, calculated using eta squared was 0.04.

Table 7-9: The affect of the Age using the ANOVA for Saudi participants

Variables	18-20		21-23		24-30				Over 40		F	eta	*p*	Different?
	Mean	SD	Mean	SD	Mean	SD	Mean	SD	Mean	SD				
IP	P value is not significant, so there are no difference													
PC_1	2.91	0.45	3.12	0.56	3.02	0.43	3.29	0.45	3.04	0.47	6.075	0.05	0.00	Moderate Difference
PC_2	P value is not significant, so there are no differences													
IT_1														
IT_2														
RB	3.74	041	3.68	0.45	3.75	0.44	3.82	0.35	3.46	0.54	2.69	0.02	0.03	Small Difference
DN	P value is not significant, so there are no differences													
IR														
ITS														

Table 7-10: The affect of the Age using the ANOVA for Malaysian participants

Variables	18-20		21-23		24-30				Over 40		F	eta	*p*	Different?
	Mean	SD	Mean	SD	Mean	SD	Mean	SD	Mean	SD				
IP	P value is not significant, so there are no differences													
PC_1														
PC_2	3.35	0.51	3.35	0.44	3.32	0.46	3.43	0.66	3.96	0.08	2.97	0.03	0.02	Small Difference
IT_1	P value is not significant, so there are no difference													
IT_2														
RB														
DN														
IR	3.69	0.42	3.53	0.50	3.57	0.49	3.71	0.35	4.00	0.00	3.38	0.04	0.01	Moderate Difference
ITS	P value is not significant, so there are no differences													

7.4 CONTINGENCY ANALYSIS

In order to investigate further the effect of nationality and gender factors on the privacy perspectives of Saudi and Malaysian participants, a contingency analysis was conducted to examine these three categorical variables: nationality gender and age. This particular piece of research explored and compared the online privacy perspectives of Saudi and Malaysian participants. It also compared the influence of gender on online privacy perspectives for each nationality. For this purpose the researcher divided, by nationality and gender, all the 47 items about online personal information, online privacy concerns and trust (independent variables) as well as all the 16 items about online privacy attitudes (dependent variables) mentioned earlier (in Chapters 5 and 6).

The analysis for this part of the research used both contingency tables and chi-square tests of independence. The contingency table was used to examine the relationship between two variables by analysing those simultaneously using percentages as a form of comparison whereas the chi-square test is used to examine how confident one can be about this relationship between these two variables occurring in the population. The value of chi-square, however, means nothing without its associated statistical significance (p <0.05), which means that the probability that the evidence of the relationship should be rejected is less than 5 chances in 100 cases (Bryman, 2008, pp.326-335). Although the items of each variable have been measured using a Likert scale as ordinal data in the questionnaire, these items were calculated in the analysis stage to become an interval data (Norman, 2010).

7.4.1 ONLINE PRIVACY PERSPECTIVES

The online privacy perspective, as mentioned in the previous chapter, consists of five main independent variables that form the individual's online privacy perspective. These are:

- the Internet user's view about what constitutes personal information (Online Personal Information PI);
- the Internet user's concerns about submitting personal information online (Privacy Concerns 1);
- the possible unexpected, unauthorized or improper secondary use of the submitted personal information (Privacy Concerns 2);
- the Internet user's concerns about handling personal information online (Internet Trust 1);
- the Internet user's concerns about the safe exchange of information with others online (Internet Trust 2).

In the next sections, a comparison of Saudi and Malaysian participants and their genders with regard to their online privacy perspectives (independent variables) is described.

7.4.2 ONLINE PERSONAL INFORMATION

A contingency analysis followed by a Pearson chi-square test (Table 7.11) indicated that when using the Internet, Malaysian participants consider their first name, e-mail address, date of birth, nationality and religion as personal information more than Saudi participants, who tend to consider the home address, phone number, photographic image and credit card number to be personal information. Malaysian male participants

considered home address and phone number to be personal information more than female participants who considered email address and nationality as personal information more than Malaysian males. Finally, female Saudi participants considered home address and photographic image to be personal information more than male participants.

Table 7-11: Comparison of participants in terms of nationality, gender and age group with regard to what is considered to constitute personal information online

First: Comparison of Malaysian and Saudi Participants				
	Malaysian (%)	Saudi (%)	Chi-square	Significance (*p*)
First Name	65	41	53.98	0.000
E-mail Address	70	41	72.647	0.000
Home Address	53	72	29.92	0.000
Phone Number	51	70	38.04	0.000
Date of Birth	62	32	84.13	0.000
Photographic Image	56	69	23.09	0.000
Credit Card Number	44	72	78.167	0.000
Nationality	57	27	108.285	0.000
Religion	62	29	118.156	0.000
Second: Comparison of Male and Female Malaysian Participants				
	Male (%)	Female (%)	Chi-square	Significance (*p*)
E-mail Address	61	73	7.315	0.026
Home Address	68	48	10.858	0.004
Phone Number	62	47	7.360	0.025
Credit Card Number	57	41	7.982	0.018
Nationality	47	61	7.647	0.022
Third: Comparison of Male and Female Saudi Participants				
	Male (%)	Female (%)	Chi-square	Significance (*p*)
Home Address	63	80	14.646	0.001
Photographic Image	50	86	71.163	0.000
Credit Card Number	65	78	17.43	0.000
Phone Number	58	81	30.26	0.000
Date of Birth	40	28	9.017	0.011
Nationality	35	18	23.376	0.000
Religion	38	21	20.722	0.000

7.4.3 PRIVACY CONCERNS 1

Contingency analysis and the Pearson chi-square test show that Malaysian participants were more likely than Saudi participants to be concerned when they submit personal information via e-mails, Social Network, Instant Messaging, Search Engines and E-government (Table 7.12). Additionally male Malaysian participants were more likely, compared to their female peers, to be concerned when they submit personal information via Search Engines and Social Network websites. Female Malaysian participants were more concerned about submitting personal information via Instant Messaging and e-government websites. The Pearson chi-square suggests that Saudi males were more concerned about submitting their personal information via the online game website compared to Saudi females (Table 7.12).

Table 7-12: Comparison of nationality, gender and age group of the participants in Privacy Concerns

First: Comparison of Malaysian and Saudi Participants				
	Malaysian (%)	Saudi (%)	Chi-square	Significance (*p*)
E-mail	81	40	131.688	0.000
Search Engines	52	35	43.374	0.000
Social Networks	68	35	94.016	0.000
Newspaper sites	48	32	27.533	0.002
Instant Messaging	69	45	65.800	0.000
Video Sharing	42	32	17.377	0.000
Live TV	45	31	28.7	0.000
Online Banking	55	53	8.59	0.000
E-Government website	62	58	19.509	0.000
Second: Comparison of Male and Female Malaysian Participants				
	Male (%)	Female (%)	Chi-square	Significance (*p*)
Search Engines	64	48	6.274	0.043
Social Network	79	64	8.181	0.017
Instant Messaging	62	72	7.783	0.020
Online Game	41	33	6.573	0.038
Video Sharing	47	42	6.148	0.046
Third: Comparison of Male and Female Saudi Participants				
Online Game	37	29	10.312	0.000

7.4.4 PRIVACY CONCERNS 2

According to the contingency analysis, the level of concerns about the destination of the submitted personal information was high among both Malaysian and Saudi participants with a mean of 73% for Saudi participants and 78.5% for Malaysian participants. The Pearson chi-square test, however, suggested that there was no significant difference between Malaysian and Saudi participants from this perspective. There was also no significant difference between male and female Malaysian participants, although the level of concern was considered high for both genders with a mean of almost 78% for female participants and more than 80% for male participants who share the same perception. Interestingly, the Saudi female participants were more likely than males to be concerned about the destination of the submitted online personal information. Nevertheless, the level of concern was considered high for both genders with a mean of more than 78% for females and 69% for males who were concerned about the destination of their online personal information (Table 7.13).

Table 7-13: Comparison of Male and Female Saudi participants' concerns about the unauthorized use of personal information submitted

First: Comparison of Malaysian and Saudi Participants				
It may …	Malaysian (%)	Saudi (%)	Chi-square	Significance (*p*)
be misused	87	74	25.375	0.00
be found by others	85	79	17.939	0.00
be used by others	84	82	50.115	0.00
be used in a way I did not expect	84	77	28.496	0.00
be used in a way I am not comfortable with	87	76	27.842	0.00
be used in a way that threatens my security	86	80	29.450	0.00
be used in a way that invades my privacy	86	79	40.883	0.00
be used in a way that could create unexpected problems	79	81	26.336	0.00
Second: Comparison of Male and Female Saudi Participants				
It may …	Male (%)	Female (%)	Chi-square	Significance (*p*)
be misused	75	86	14.083	0.009
be found by others	67	81	11.529	0.003
be used in a way I did not expect	77	87	6.981	0.030
be used in a way I am not comfortable with	73	82	9.645	0.008
be used in a way that threatens my security	73	80	7.092	0.009
be used in a way that invades my privacy	75	86	10.819	0.004
be used in a way that could create unexpected problems	67	82	10.650	0.005

7.4.5 INTERNET TRUST 1 - PROFESSIONAL HANDLING

Contingency analysis and the Pearson chi-square test showed that Malaysian participants tended to trust the professional handling of e-mails, Instant Messaging and Social Networks websites in protecting their personal information more compared to Saudi participants whereas the latter have more confidence in a site's professionalism when video sharing and using online banking websites to submit personal information (Table 7.14). Additionally, male Saudi participants were more likely to trust the

professional handling of their information on online banking websites compared with their female peers. Nevertheless, the Pearson chi-square suggests that there is no significant difference between male and female Malaysian participants with regard to their trust in Internet websites to handle their personal information online (Table 7.14).

Table 7-14: Comparison of nationality, gender and age group of the participants in terms of trust in the professional handling of their information online

First: Comparison of Malaysian and Saudi Participants				
	Malaysian (%)	Saudi (%)	Chi-square	Significance (*p*)
E-mail	76	52	47.983	0.00
Search Engines	31	31	11.021	0.044
Social Networks	36	29	11.364	0.00
Newspaper sites	37	30	15.369	0.00
Instant Messaging	43	34	21.502	0.00
Video Sharing	15	17	7.584	0.04
Live TV	25	22	12.692	0.005
Online Banking	54	63	6.622	0.036
Second: Comparison of Male and Female of Saudi Participants				
	Male (%)	Female (%)	Chi-square	Significance (*p*)
Online Banking	65	55		0.027

7.4.6 INTERNET TRUST 2 – INFORMATION SECURITY

According to the contingency analysis, Malaysian participants are more likely compared to Saudi participants to trust the security of the exchange of their personal information via e-mails, Instant Messaging, social networks, newspaper and video sharing websites (Table 7.15). Saudi male participants are more likely compared to females to trust online game websites when exchanging their personal information.

Table 7-15: Comparison of nationality, and gender of the participants in privacy trust – information security

First: Comparison of Malaysian and Saudi Participants				
	Malaysian (%)	Saudi (%)	Chi-square	Significance (*p*)
E-mail	67	54	17.787	0.00
Social Networks	34	22	24.198	0.00
Newspaper sites	30	21	24.302	0.00
Instant Messaging	40	39	7.201	0.027
Online Games	11	13	12.948	0.002
Video Sharing	14	10	30.263	0.00
Second: Comparison of Male and Female of Saudi Participants				
	Male (%)	Female (%)	Chi-square	Significance (*p*)
Online Games	17	9	8.96	0.009

7.4.7 CULTURAL EFFECTS ON ONLINE PRIVACY ATTITUDES

As mentioned in Chapter 5, online privacy attitudes are defined as the individual's intentions and acts to guard their personal information online, care about their privacy online, care about others' privacy online and being careful when revealing personal information. In addition, these attitudes are observed with four cultural effects, that is, dependent variables, which are Social Norms, Religious Beliefs, Internet Regulations and IT Skills effects.

There now follows a comparison of the cultural effects on the Saudi and Malaysian participants' online privacy attitudes (dependent variables) with regard to the nationality and gender.

7.4.8 THE EFFECT OF RELIGIOUS BELIEFS ON THE ONLINE PRIVACY ATTITUDES

Contingency analysis and the Pearson chi-square test showed that the effect of religious beliefs on the Saudi participants' attitude on the care about others privacy were more than Malaysian participants who were affected by religious beliefs on their attitude of

been careful when reveling personal information (Table 7.16). Additionally, female Saudi participants were more affected by religious beliefs on their online privacy attitudes compared to male participants.

Table 7-16: Comparison of nationality and gender of the participants on the effect of their religion believe in the online privacy attitudes

First: Comparison of Malaysian and Saudi Participants				
	Malaysian (%)	Saudi (%)	Chi-square	Significance (*p*)
Keeping my personal Information	74	74	21.794	0.00
I should care about my privacy	77	77	11.742	0.003
I should care about others privacy	82	89	8.963	0.011
I should be careful when revelling Personal Information	78	75	17.55	0.000
Second: Comparison of Male and Female Saudi Participants				
	Male (%)	Female (%)	Chi-square	Significance (*p*)
Keeping my personal Information	68	80	11.546	0.003
I should care about my privacy	71	84	10.474	0.005
I should be careful when revelling Personal Information	68	81	13.351	0.001

7.4.9 THE EFFECT OF THE SOCIAL NORMS ON THE ONLINE PRIVACY ATTITUDES

Contingency analysis and the Pearson chi-square test showed that the effect of social norms on the Malaysian participants on the online privacy attitudes are more compared to Saudi participants (Table 7.17). Moreover, female Saudi participants are more affected by social norms on their attitude of been careful when revealing Personal Information compared to male participants (Table 7.17).

Table 7-17: Comparison of nationality and gender of the participants on the effect of their social norms in the online privacy attitudes

First: Comparison of Malaysian and Saudi Participants				
	Malaysian (%)	Saudi (%)	Chi-square	Significance (*p*)
Keeping my personal Information	93	71	59.375	0.00
I should care about my privacy	92	71	51.734	0.00
I should care about others privacy	91	43	37.461	0.00
I should be careful when revelling Personal Information	89	64	62.107	0.00
Second: Comparison of Male and Female Saudi Participants				
	Male (%)	Female (%)	Chi-square	Significance (*p*)
I should be careful when revelling Personal Information	59	70	6.219	0.045

7.4.10 THE EFFECT OF THE INTERNET REGULATION ON THE ONLINE PRIVACY ATTITUDES

Contingency analysis and the Pearson chi-square test showed that the effect of local Internet regulation on the Malaysian participants on their online privacy attitudes were more than Saudi participants (Table 7.18).

Table 7-18: Comparison of nationality and gender of the participants on the effect of the local Internet regulation in the online privacy attitudes

First: Comparison of Malaysian and Saudi Participants				
	Malaysian (%)	Saudi (%)	Chi-square	Significance (*p*)
Keeping my personal Information	62	54	21.335	0.00
I should care about my privacy	64	60	7.010	0.030
I should care about others privacy	70	64	9.494	0.009
I should be careful when revelling Personal Information	69	58	28.012	0.000

7.4.11 THE EFFECT OF THE IT SKILLS ON THE ONLINE PRIVACY ATTITUDES

Contingency analysis and the Pearson chi-square test showed that the effect of IT skills on the Malaysian participants on their online privacy attitudes were more compared to Saudi participants. The contingency analysis also showed no differences in gender diversity.

Table 7-19: Comparison of nationality and gender of the participants on the effect of the IT skills in the online privacy attitudes

First: Comparison of Malaysian and Saudi Participants				
	Malaysian (%)	Saudi (%)	Chi-square	Significance (*p*)
Keeping my personal Information	66	58	11.582	0.003
I should care about my privacy	67	62	8.232	0.020
I should care about others privacy	67	60	7.740	0.021
I should be careful when revelling Personal Information	68	57	19.644	0.000

7.4.12 SUMMARY OF THE EFFECTS OF NATIONALITY, GENDER AND AGE ON THE PRIVACY PERSPECTIVE

In summary, more Malaysian participants consider name, e-mail address, date of birth, nationality and religion as personal information more compared to Saudi students. In addition, Malaysian participants considered that submitting the abovementioned personal information via e-mails, instant messaging and search engines websites was a privacy concern. They, however trust both the professional handling of their personal information and the security of exchanging this information via the same activities, that is, e-mails and instant messaging as well as social networks websites more than the

Saudi participants. Furthermore, Malaysian participants were more likely to be motivated by their family and friends and Internet regulation in Malaysia in their attitude towards taking care over their personal information as well as others' personal information online. Moving to gender differences among Malaysian participants, male and female Malaysians almost coincided in their consideration of what constitutes personal information. Their home addresses and phone numbers, however, were considered personal information from the male point of view but this was not the case for female participants. Regarding the age factor, for Malaysian participants, age tends to play a role in decreasing the effect of religious beliefs, family and friends on, respectively, the Malaysian view of the importance of guarding and caring for their personal Information.

Saudi participants, on other hand, tended to consider home address, phone number, photographic image and credit card number as personal information more than Malaysian participants; however, their level of privacy concerns and online trust were lower than that of the Malaysian. In addition, the Saudi participants' attitudes about guarding their personal information were driven by their religious beliefs more than the Malayans. With regard to the role of gender, Saudi female participants considered their home address and photographic image to be more personal information than male participants do. Both female and male participants in Saudi Arabia had the same level of privacy concerns. Male participants, however, were more likely to trust the professional handling of their information and the security of exchanging this information by e-mail, online games, video sharing and live TV websites than their female peers. In addition, male participants tended to be affected more by their family and friends, Internet

regulation and their IT skills in their attitude towards guarding personal information, whereas female participants were affected more by their religious beliefs in their attitudes towards the importance of caring about their personal information. Regarding the impact of the age factor on Saudi participants' perspectives, older Saudi participants were more likely compared to young participants to consider their first and full name and date of birth as personal information. In addition, older Saudi participants were more concerned with regard to submitting personal information via e-mails and websites and had greater privacy concerns about submitting personal information using social network websites but they trusted e-commerce websites with the professional handling of their personal information.

7.5 CONCLUSION

In this chapter, the effects of nationality, gender and age factors on online privacy concerns and trust and the online privacy attitude, were analysed using both contingency tables and chi-square tests of independence. In addition, this chapter has demonstrated an inferential data analysis for the survey data from both Saudi Arabia and Malaysia using simple linear regression analysis. The results have helped to answer the study's research question and identified the cultural influences that affect the privacy perspectives of the individual Saudi and Malaysian Muslims in their internet usage, as well as the similarities and differences between these perspectives.

8 CHAPTER 8: THE DISCUSSION

8.1 INTRODUCTION

This study investigates the relationship between the privacy perspectives of Internet users, the four cultural effects on online privacy attitudes and the three demographic factors: nationality, age and gender, which are represented on the research model (see section 5.2). In Chapter 7, an advanced analysis was conducted on the data collected from both Saudi Arabian and Malaysian participants in order to answer the research questions of this study and identify the cultural influences that affect the privacy perspectives of individual Saudi and Malaysian Muslims in their internet usage and identify the similarities and differences between these perspectives. In order to achieve these aims, Chapter 7 tested the research hypotheses constructed to study the relationship between the privacy perspective of Internet users and the four cultural effects by using simple linear regression analysis. The analysis also illustrated the effect of nationality, gender and age factors on online privacy concerns, trust and the online privacy attitude by using t-test, ANOVA and contingency tables with chi-square tests of independence.

This chapter summarises the main outcomes of the empirical research, that is, the t-test, ANOVA, contingency and simple linear regression analyses. The chapter discusses these findings in the context of the relevant literature, particularly from the perspective of the importance of privacy. The discussion considers the issue from the psychological and sociological stand -points, the factor involved in measuring information privacy and from the qualitative data collected via the open questions included in the questionnaire.

In this chapter, a comparison between the Malaysian and Saudi participants with regards to their perception of online privacy concerns and Internet trust will be illustrated. Moreover, the differences of the effect of the cultural (religious beliefs, social norms, Internet regulation and the IT skills) and demographic (age, gender and nationality) factors on online privacy attitudes will be demonstrated.

This chapter is divided into three main sections. The first section is a summary and comparison of the effect of nationality, gender, age and cultural backgrounds including Religious Belief (RB), Social Norms (SN), Internet Regulation (IR) and IT Skills (ITS) on the five online privacy perspective concerns of both Malaysian and Saudi participants. These issues are: Internet user's concerns about submitting personal information online (PC-1); their concerns about the possible unexpected, unauthorised or improper secondary use of the submitted personal information (PC-2); Internet trust including the Internet user's concerns regarding the disclosure of personal information online (IT-1); the Internet user's trust regarding the safety of the exchange of information with others online (IT-2). The second section of this chapter is a summary of and comparison between the effect of the nationality, gender and age on the cultural backgrounds including the religious belief (RB), social norms (SN), Internet regulation (IR) and IT skills (ITS) on both Malaysian and Saudi participants. Then the third section is a discussion involving the results of testing the research hypotheses and by highlighting the differences between Malaysian and Saudi participants.

8.2 ONLINE PRIVACY PERSPECTIVES

The online privacy perspective was mentioned in Chapters two and five. It consists of the privacy concern (PC), Internet trust (IT) and the type of personal information (PI) (Figure 8.1). Moreover, the privacy concern includes the Internet users' concerns about submitting personal information online (PC-1) and their concerns about the possible unexpected, unauthorised or improper secondary use of the personal information submitted (PC-2). Internet trust includes the Internet user's concerns regarding the disclosure of personal information online (IT-1) and the Internet user's trust regarding the safety of the exchange of information with others online (IT-2) (Smith *et al.*, 1996, p.189 and Dinev and Hart, 2006, pp.63-64).

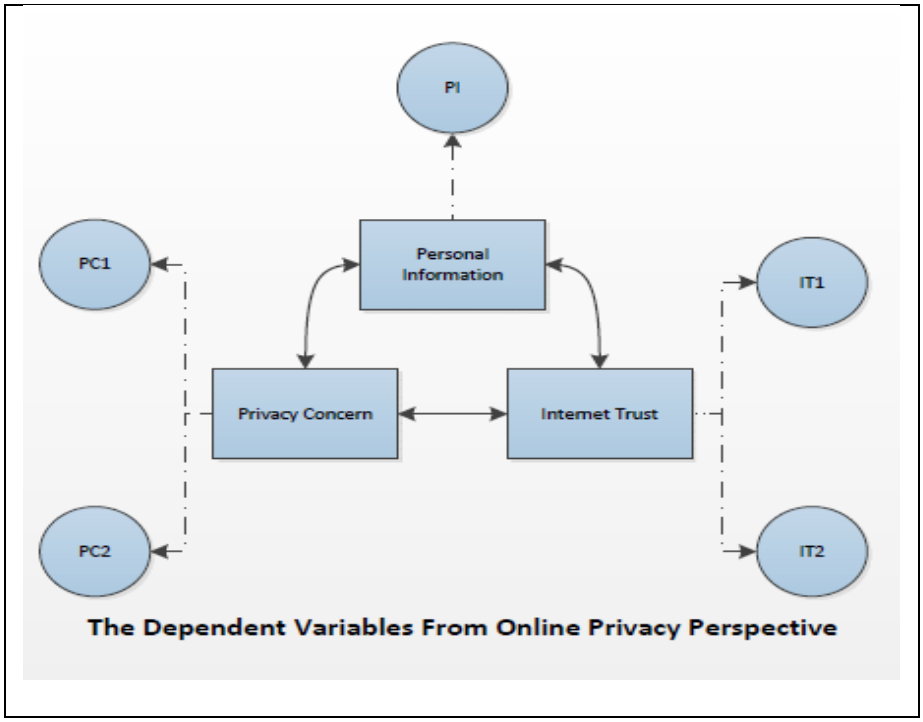


Figure 8-1: The Five Dependent Variables for the Online Privacy Perspective

The effect of nationality, gender and age on each item of the PI, PC-1, PC-2, IT-1 and IT-2 was reported in chapter 7. The effect of the cultural backgrounds including religious beliefs (RB), social norms (SN), Internet regulation (IR) and IT skills (ITS) on

the PC-1, PC-2, IT-1 and IT-2 were reported in the same chapter. The current chapter summarises of the effect of these factors upon the relevant components of the online privacy perspectives in order to highlight the differences and similarities between the Malaysian and Saudi participants.

8.2.1 ONLINE PERSONAL INFORMATION

The online personal information variable was included in the questionnaire (as mentioned in Chapter 5) to prepare the participants for the following questions. The question associated with this variable provided the participants with a list of what online personal information might consist of. This question aimed to investigate the similarities and differences between Malaysian and Saudi participants regarding what they considered personal information. In order to analyze the data that was collected from this question, contingency tables with a chi-square test were used to examine the differences between Malaysia and Saudi (males and females of different age groups) with regard to their perspective on the 11 items of what were considered questions requiring personal information to be divulged. These items were first name, full name, e-mail address, home address and phone number, date of birth, photographic image, credit card number, nationality, religion and political views.

With regard to the effect of nationality on what is considered as personal information, the findings in Chapter 7 showed that most Malaysian participants consider their name, e-mail address, date of birth, nationality and religion personal information when they use the Internet (Figure 8.2). These five items of personal information could be

categorized, according to Guarda and Zannone, (2008, p.7), into personal data (name, e-mail address and date of birth) and sensitive data (nationality and religion).

With regard to the Saudi participants, the results showed that most Saudis consider their home address, phone number, photographic image and credit card number personal information when they use the Internet (Figure 8.2). These four items of personal information which are identified in this research and, also, by Al-Saggaf and Weckert (2011, pp.42) could be categorized, according to Guarda and Zannone, (2008, p.7), as personal data (home address, phone number and photographic image) and identification data (credit card number). Interestingly, less than a third of the Saudi participants considered nationality (27%) and religion (29%) personal information i.e. sensitive data. This could be due to all students in the higher education system in Saudi Arabia (with the exception of the King Abdullah University of Science and Technology (KAUST)) being Muslims and almost all of them Saudis. Therefore, they might not consider this information sensitive data as they are all similar in this respect. In the student populations in Malaysian universities there is a mixture of national and international Muslim and non-Muslim students. In addition, in Malaysia, a person's religion could be an indication of their race, i.e. the Malaysian constitution states that a Malay is a Muslim (Hirchman, 1987, p.3, and Chin, 2010, p.84), although a Malaysian Muslim could be of Arabic, Indian or Chinese origin (Cheong, *et al*, 2009, p.41). Information about their religious affiliations would associate them with a particular group. This may set them apart from other groups that claim to be treated unfairly. For example, non-Muslims, particularly those of Chinese origin may come to feel second class citizens due to the number of rules passed by the government that seem to favour Muslims.

These rules are likely to raise questions about democracy by non –Muslims (Chin, 2010, pp.81-89).

Two of the five perspectives of privacy importance could explain the difference between the Malaysian and Saudi perceptions of what is considered personal information (Clarke 2006, pp.1-2; Kemp and Moore 2007, pp.58-77). These were the psychological perspective, which includes the ability to judge the possible threat and the social perspective, which includes the ability to be free to associate with others as desired. For example, the Malaysians consider name, email address and date of birth personal data while the Saudis consider home address, phone number and photographic image, because each of them considers what could cause a threatening situation for themselves, namely email and data of birth in Malaysia and home address and credit card in Saudi Arabia. Moreover, the Malaysians compared to the Saudis consider information about their religious affiliations personal, which could be because others, i.e. non-Muslim, find it sensitive information.

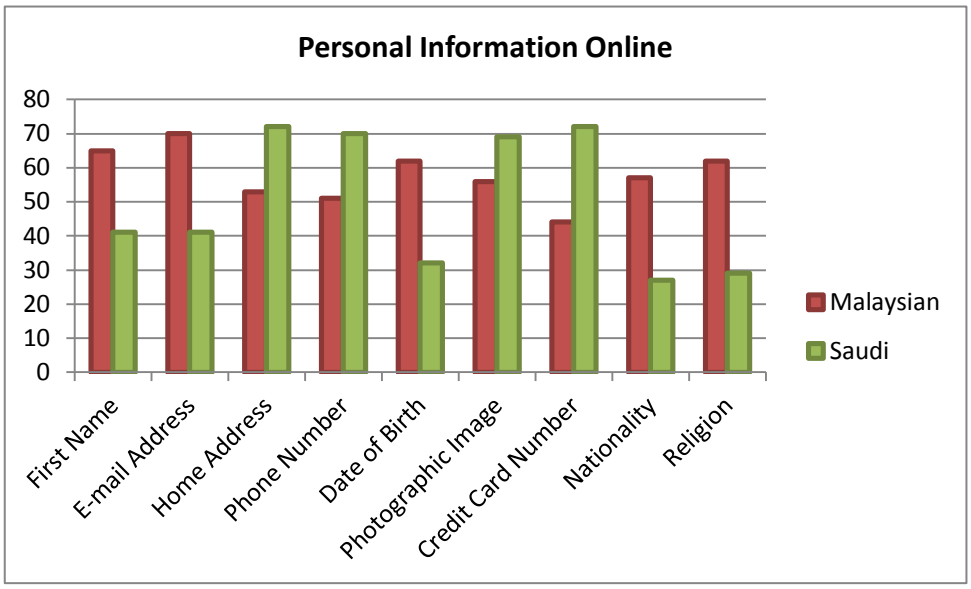


Figure 8-2: Comparison of Malaysian and Saudi participants of what is considered to constitute Personal Information online

With regards to the effect of gender on the Malaysian and Saudi perceptions of what is considered as personal information, a greater percentage of Saudi females (compared to males) considered home address, photographic image, credit card and phone number as personal information (Figure 8.3). These gender differences could be explained by the need for physical security and to be secure from harassment, which are two factors from the fourth part of the social web gendered privacy model according to Thelwall, (2011, pp.252-254). Physical security tends to be more significant for females particularly with respect to phone number and home address to avoid any violence caused by those who contact them online. With respect to freedom from harassment, females tend to worry about becoming victims of inappropriate sexual comments or having attention

inappropriately drawn to their personal appearance for example, comments about attractiveness in a photo or when presenting or when teaching her subject field[3] (Thelwall, 2011, pp.252-254)

With regard to Saudi Arabia, this result is not surprising in the light of the cultural norms and regulations of that country where the rules require females to gain a male guardian's approval for many aspects of their lives, for example, to attend university, work in government offices and travel (Al Lily, 2011, p.120). Accordingly their personal information is considered very sensitive and treated in a cautious way. For example, in September 2011, the Interior Ministry banned government offices from recording females' mobile phone numbers in their paper-work (Daralhyat.com). According to the Alhayat newspaper (dated 9 September 2011), this ban followed a previous order to government offices to record the mobile phone numbers of every person who submitted paper-work (emirate247). This was to be able to contact them by SMS with an update, however, according to the newspaper, after evaluating the pros and cons of recording females' mobile phone numbers, the Interior Ministry banned the practise. This could go along with previous researches on the gender dissimilarity with regards to providing their phone number, for example Fogel and Nehmad, (2009, p.159) notes that men tend to include their phone number on their Internet profile more than women do. Such behaviour could be, as Fogel and Nehmad explain, due to the social

[3] It is a global attitude within females.

norms that built subjective knowledge based on the face-to-face situations in which the men, more than women, are more comfortable exchanging their phone numbers.

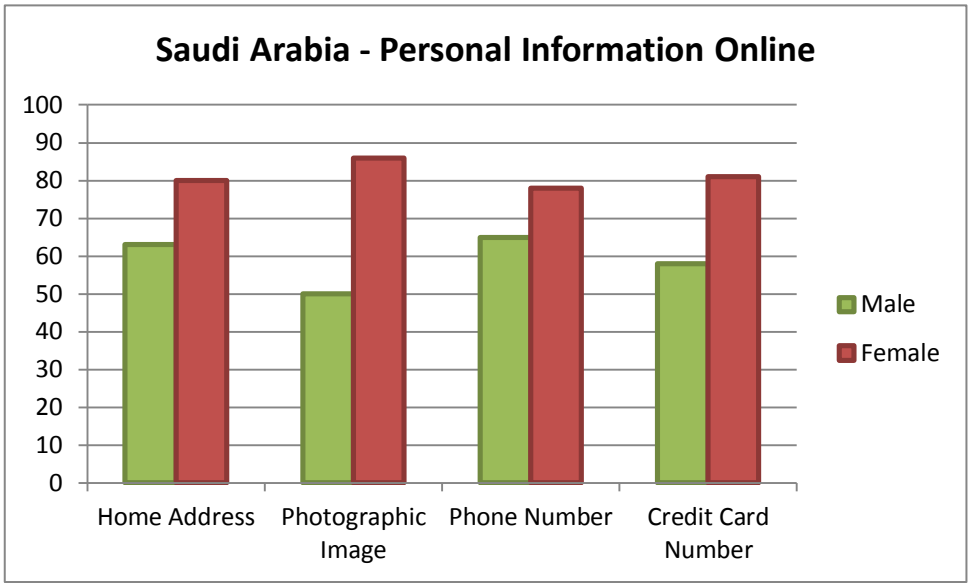


Figure 8-3: Comparison of Male and Female within Saudi participants within Saudi of what is considered to constitute Personal Information online

8.2.2 PRIVACY CONCERNS ABOUT SUBMITTING PERSONAL INFORMATION VIA THE INTERNET PC-1

In this sub-section the effect of nationality, gender, age, religious belief (RB), social norms (SN), Internet regulation (IR) and IT skills (ITS) on the privacy concerns about submitting personal information via the Internet PC-1 is discussed (Figures 8.4 and 8.5).

The nationality factor affected PC-1, as the t-test proved the existence of a moderate difference between Saudi and Malaysian participants. There was, however, no effect of the gender factor on either Malaysian or Saudi samples. This could be due to both men and women having the same perception with regards to the level of Internet users' concerns over submitting personal information online (PC-1), regardless of differences

in their perception about what is considered to be personal information, as mentioned in section (8.2.1).

The age factor was found to be another variable but it only affected the PC-1 of the Saudi sample population. The ANOVA test on the Saudi samples showed the effect of age. Zukowski and Brown (2007, p.201) statistically confirmed this phenomena when they said, "Older Internet users are more concerned about information privacy than younger Internet users". The difference may due to the digital divide of age that contributes to the lack of knowledge of the Internet's potential for collecting data from its users (Maab, 2011, p.241).

With regard to the cultural effects, the regression test proved that religious belief, social norms and IT skills were factors affecting the PC-1 in Saudi Arabia whereas social norms, Internet regulation and IT skills were found to be significantly affecting factors on the PC-1 in Malaysia. Yao (2011, p.119) states that the family tends to affect the development of its members in terms of independence and autonomy, Yao (ibid, p.121), also states that experiences would increase confidence on the Internet and therefore "reduce self-protection intention and behaviour" (ibid, p.121). Moreover, as mentioned in section (2.3.1), Internet literacy encourages awareness of the online privacy concerns among Internet users (Dinev and Hart, 2006, p.9). Therefore it is no surprise to identify social norms and IT skills as common effects on the privacy concerns of both Malaysian and Saudi participants.

In addition the combination of the effect of the social norms and religious beliefs on the privacy concerns (PC-1) among the Saudi participants suggests that these two effects could be considered to be related effects given that in Saudi Arabia, religion, i.e. Islam is a part of the definition of Saudi culture and therefore plays a major role in the shaping of the social norms in Saudi Arabia (Al-Saggaf, 2004, p.1).

Finally, with regards to the effect of Internet regulation on privacy concerns (PC-1) in Malaysia and Saudi Arabia, although both countries have a poor records of privacy protection due to the lack of right to privacy in their constitution (Ho, *et al*, 2010, p.3 and Al Ghaith, *et al*, 2010, p.7), in Malaysia - unlike in Saudi Arabia the participants' privacy concerns appear to be affected by the Internet regulation in the country. This could be due to the Personal Data Protection Act 2009 which is still awaiting approval (Ho, *et al*, 2010, p.6, and Hasbullah et al, 2011, p.311).

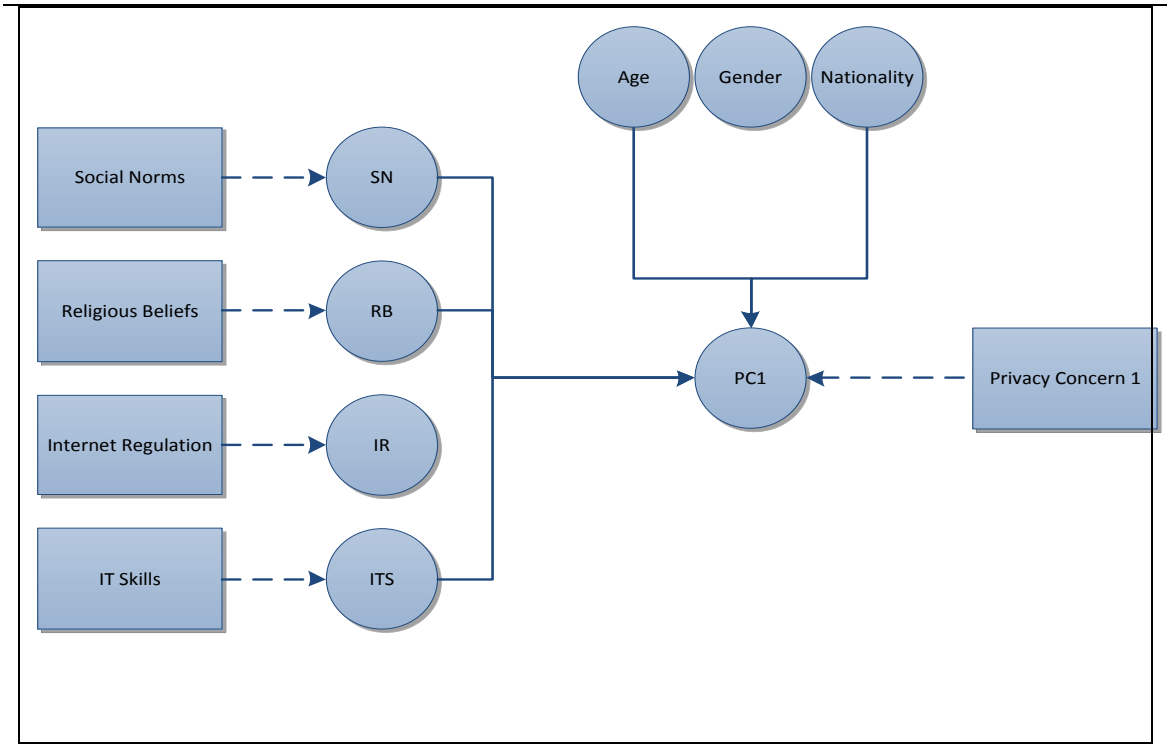


Figure 8-4:The effect of Saudi nationality, gender, age and cultural background including the religious beliefs, social norms, Internet regulation and IT skills on the privacy concern about submitting personal information via the Internet PC-1

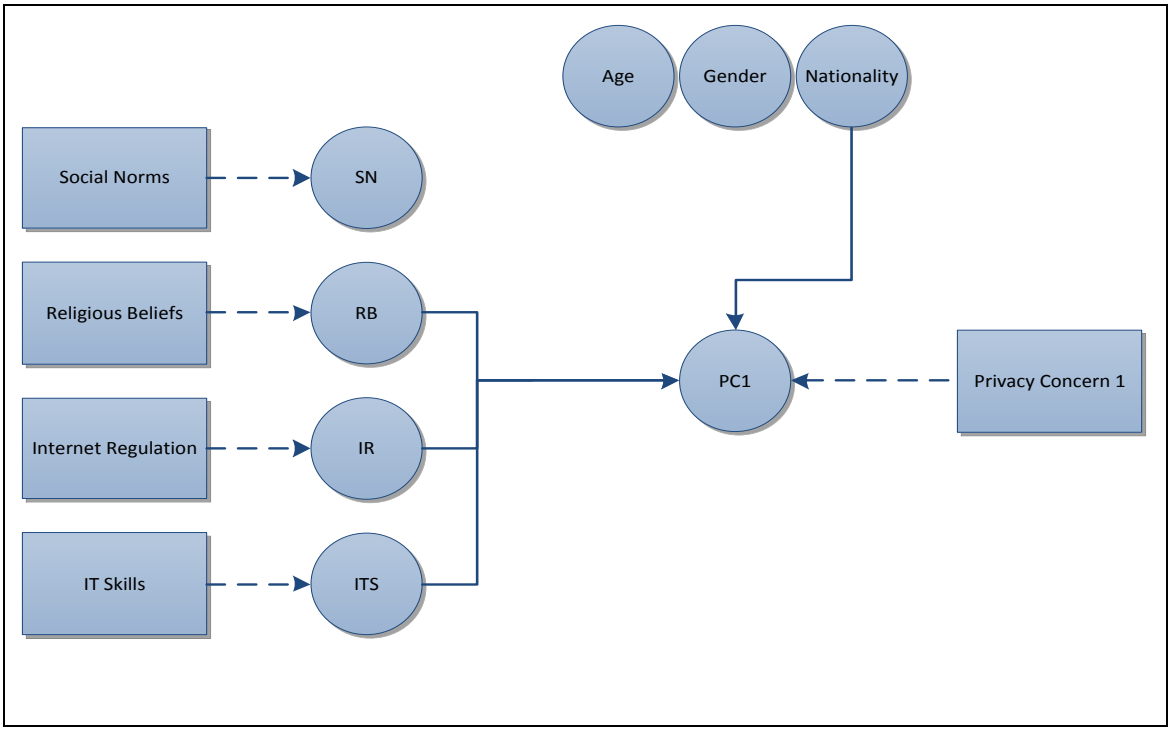


Figure 8-5: The effect of Malaysian nationality, gender, age and cultural background including the religious beliefs, social norms, Internet regulation and IT skills on the privacy concern about submitting personal information via the Internet PC-1

More details on the effect of nationality on the privacy concerns about submitting personal information via the Internet PC-1 were reported in Chapter 7, in which these effects were tested on each of the 11 Internet websites included in the study. The following is a summary of the effect of these factors on the PC-1 (Figure 8.6).

Malaysian participants were more likely to be concerned than their Saudi counterparts were when they submitted personal information via e-mails and Instant Messaging. In addition, some Malaysian participants showed concerns about their privacy when they used e-mail because of the possibility of receiving junk mail or SPAM, particularly those with phishing intentions. For example, in answering a question about what could affect their trust in their online privacy, one said that they would be wary. "There is too much spam in my e-mail inbox." Another one said he, "Got a few junk e-mails." Another said, "When weird e-mails got sent to my e-mail then I knew my information was abused somewhere." Saudi *et al*, (2007, p.82) stated that SPAM emails are considered the most common method of online phishing and 29% of the Internet users in Malaysia blamed the vendor for causing these phishing SPAMs.

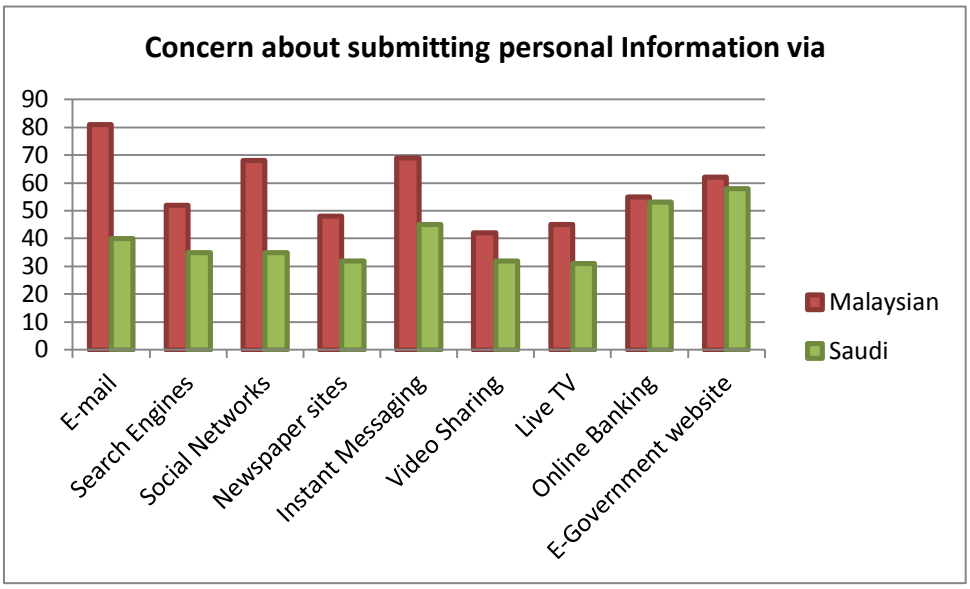


Figure 8-6: Comparison of Malaysian and Saudi participants with regard to activities associated with privacy concerns PC-1

8.2.3 PRIVACY CONCERNS OVER THE POSSIBLE UNEXPECTED, UNAUTHORISED OR IMPROPER SECONDARY USE OF SUBMITTED PERSONAL INFORMATION PC-2

The following discussion details the effect of nationality, gender, age, religious belief (RB), social norms (SN), Internet regulation (IR) and IT skills (ITS) on the privacy concerns about the possible unexpected, unauthorised or improper secondary use of the submitted personal information PC-2 (Figures 8.7 and 8.8).

The nationality factor was found to affect PC-2. The t-test on nationality and PC-2 proved the existence of a small difference between the Saudi and Malaysian participants. In addition the differences between Saudi and Malaysian participants with regard to their privacy concerns over the possible unexpected, unauthorised or improper secondary use of their submitted personal information PC-2 could be explained by differences in cultural effects, which come from religious belief and IT skills. These are

the cultural effects that act on PC-2 in Saudi Arabia while social norms and Internet regulation are the cultural effects that act on PC-2 in Malaysia.

The gender factor had no effect on Malaysian participants and only a small one on Saudi participants. This gender difference over privacy concerns about the possible unexpected, unauthorised or improper secondary use of their submitted personal information submitted, PC-2, could be because females have significantly more concerns than males in the perception of the privacy concerns (Fogel and Nehmad, 2009, p.157), which could explain the act of Saudi authority, as mentioned in 8.2.1, by which government offices have been banned from recording females' mobile phone numbers in their paperwork (Daralhyat.com).

Using the ANOVA test, the age factor, was found to have a small effect on the Malaysian participants and no effect on the Saudi participants, as mentioned in section (8.2.2). The age factor effects on the concerns about online information privacy and could be as a consequence of the digital age divide (Zukowski and Brown, 2007, p.201 and Maab, 2011, p.241).

Interestingly, whilst the effect of age on the privacy concerns about submitting personal information via the Internet PC-1 is proven with the Saudi participants it is not proven with the Malaysian participants. This suggests that in Saudi Arabia, the different age groups are dissimilar in their concerns with regards to the act of submitting personal information online, however they are the same with regards to the concerns about what happens to the personal information.

In addition, the reverse is true with the effect of age on privacy concerns over the possible unexpected, unauthorised or improper secondary use of the submitted personal information PC-2, in which age affects the privacy concern of the Malaysian cases and does not affect on the Saudi cases. This suggests that in Malaysia, the different age groups are similar in their concerns with regards to the act of submitting personal information online, however they are not the same with regards to the concerns about what happens to this personal information. This could be explained by the existence of the effect of Internet regulation on the Malaysian cases but not the Saudi cases which suggested that all different age groups in Malaysia are aware of the Internet regulation. This enables them to form an early perception on how their personal information would be treated when they submit it.

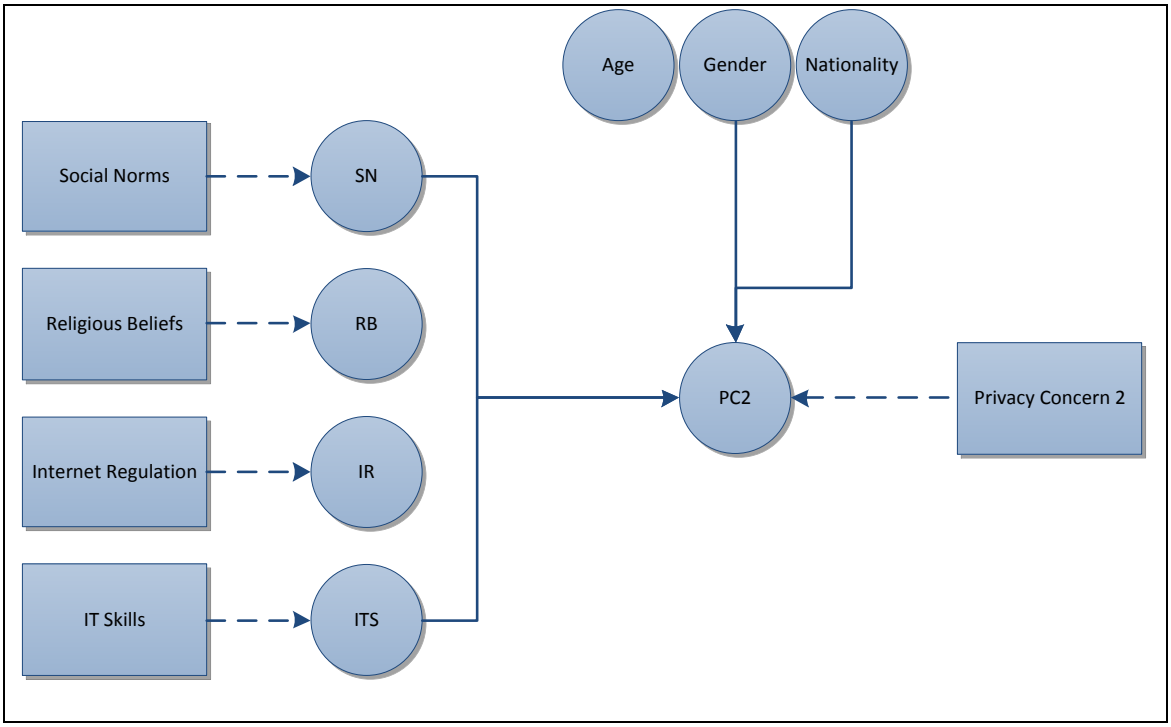


Figure 8-7: The effect of the Saudi nationality, gender, age and cultural backgrounds including religious belief, social norms, Internet regulation and IT skills on the privacy concern about the unauthorized use of submitted personal information PC-2

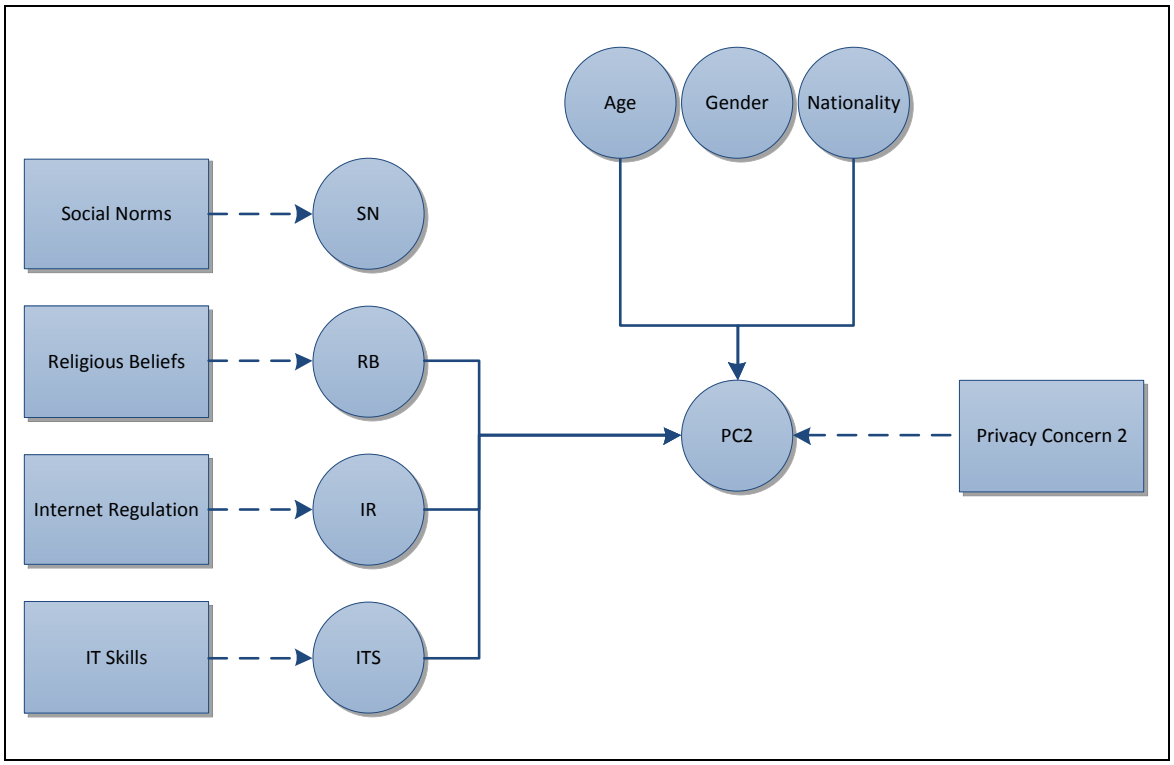


Figure 8-8:The effect of the Malaysian nationality, gender, age and cultural backgrounds including religious belief, social norms, Internet regulation and IT skills on the privacy concern about the unauthorized use of submitted personal information PC-2

8.2.4 TRUST IN THE PROFESSIONAL HANDLING OF PERSONAL INFORMATION VIA THE INTERNET IT-1

The effect of the nationality, gender, age, religious belief (RB), social norms (SN), Internet regulation (IR) and IT skills (ITS) on the trust of the professional handling of personal information via the Internet IT-1, is discussed in the following section (Figures 8.9 and 9.10).

The nationality factor was found to affect IT-1. The t-test on the nationality factor and IT-1 proved the existence of a very small difference between the Saudi and Malaysian participants. The gender factor was found to have no effect on Malaysian participants while it affected Saudi participants slightly. The t-test showed that there was a small

difference between Saudi males and females. The age factor was found, using an ANOVA test, to have no effect on either Saudi or Malaysian participants.

With regard to cultural effects, the regression test proved that religious belief, social norms and IT skills affected IT-1 in Saudi Arabia while religious belief, social norms, Internet regulation and IT skills affected IT-1 in Malaysia.

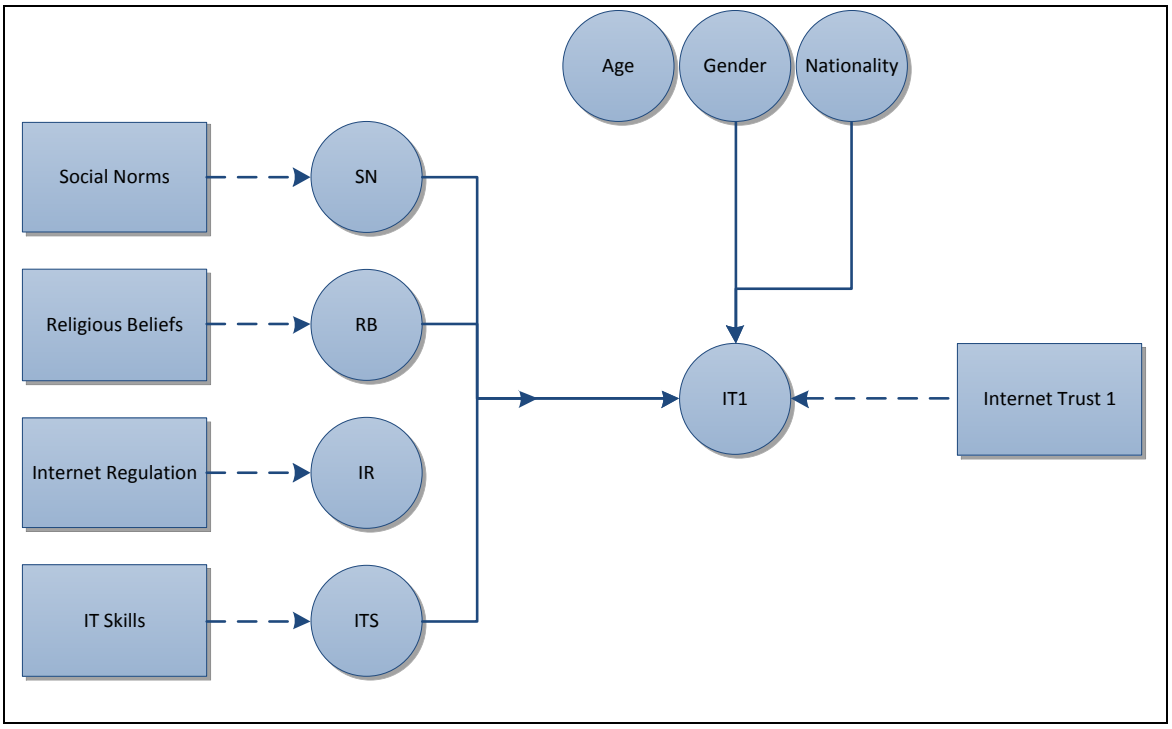


Figure 8-9: The effect of the Saudi nationality, gender, age and cultural backgrounds including religious belief, social norms, Internet regulation and IT skills on the trust in the professional handling of their information in various online activities IT-1

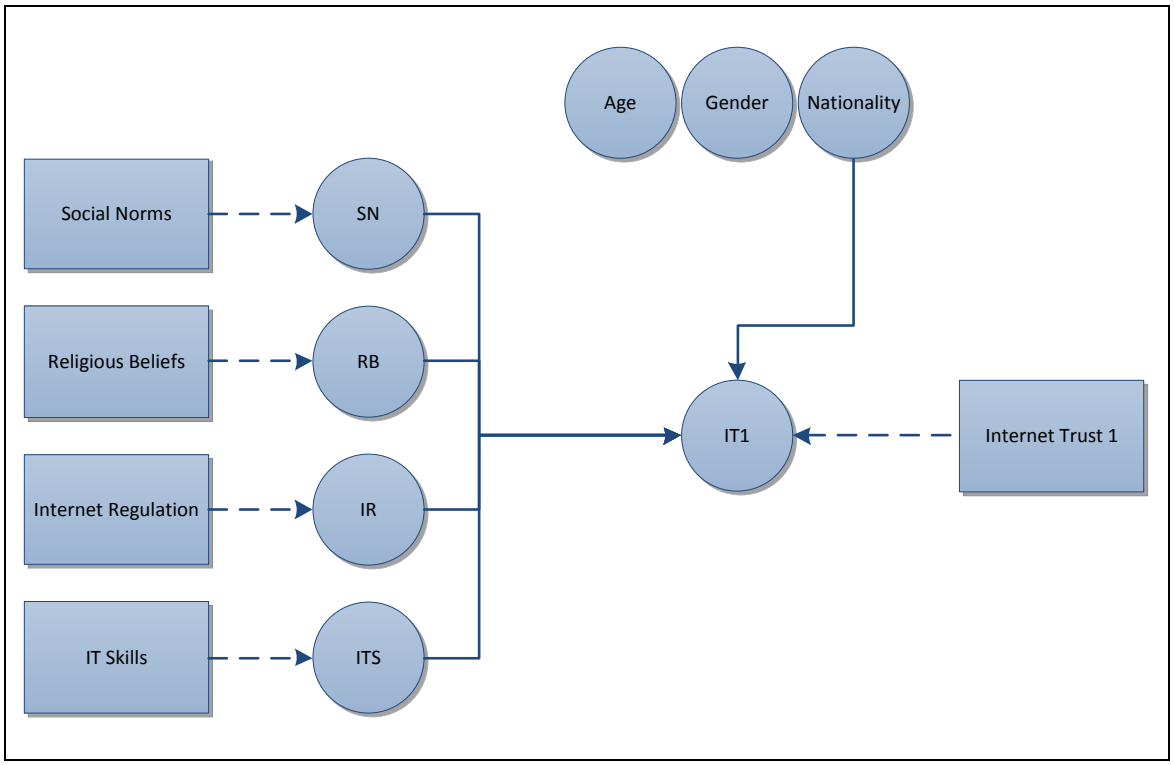


Figure 8-10: The effect of the Malaysian nationality, gender, age and cultural backgrounds including religious belief, social norms, Internet regulation and IT skills on the trust in the professional handling of their information in various online activities IT-1

More details on the effect of nationality on the trust in the professional handling of their information in various online activities IT-1were reported in Chapter 7. The nationality factor was tested on each of the 11 Internet websites included in the study. Malaysian participants showed that they trusted the professional handling of e-mails, Instant Messaging and Social Networks websites to protect their personal information compared to Saudi participants who trusted more the professionalism of online banking websites to handle their personal information safely (Figure 8.11).

Interestingly, Malaysian participants expressed their concern about submitting personal information via e-mails; however, they seem to trust email websites to handle their personal information professionally. In addition, Saudi participants considered their

credit card number personal information and yet were willing to rely on the professionalism of online banking websites to secure their private details. This result could have arisen because whilst concerns about privacy are raised, an interest in understanding the act of informational detection during data collection are raised as well, particularly in order to be able to measure information privacy (Lee and Kwon 2010, p.5194) and, therefore, the willingness be able to trust the website that is collecting the data. This speculation needs further investigation in order to examine the relationship between the level of privacy concerns while using communication websites and the level of trust in their professionalism.

According to the results of the contingency analysis and the Pearson chi-square test, Malaysian participants were more likely (81%) than Saudi participants (40%) to be concerned when they submit personal information via e-mails. So with comparing to Saudis, Malaysian participants are more concerned about submitting personal information via e-mails.

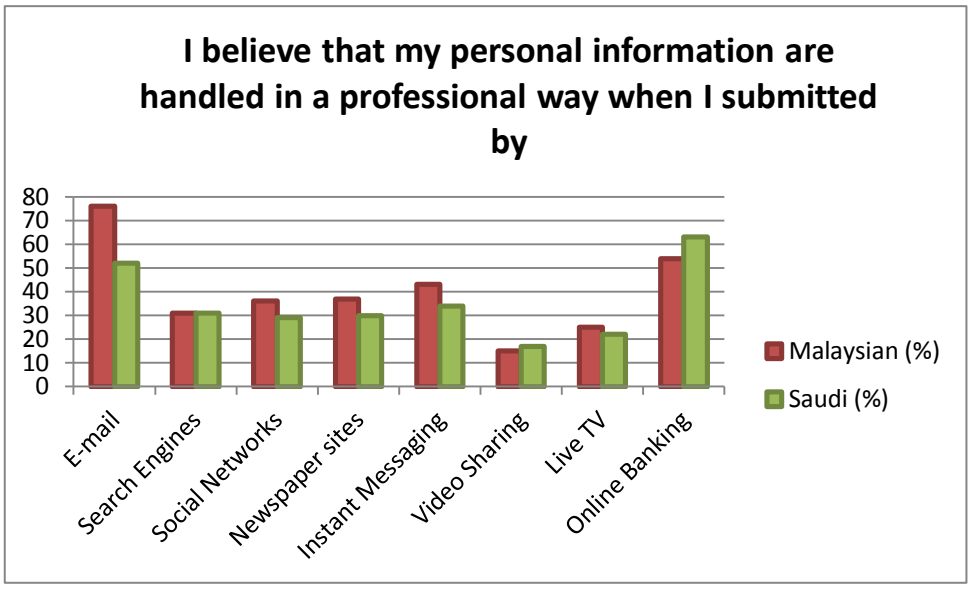


Figure 8-11:Comparison of Malaysian and Saudi participants with regards to trust in the professional handling of their information in various online activities

8.2.5 THE TRUST IN THE SAFE EXCHANGE OF ONE'S PERSONAL INFORMATION VIA THE INTERNET IT-2

In this sub-section, the details of the effect of nationality, gender, age, religious belief (RB,) social norms (SN), Internet regulation (IR) and IT skills (ITS) on trust in the safe exchange of one's personal information via the Internet IT-2 are discussed (Figures 8.12, 8.13 and 8.14).

The nationality factor was found to affect trust in the safe exchange of one's personal information via the Internet IT-2. The t-test on nationality and IT-2 proved the existence of a small difference between the Saudi and Malaysian participants. The gender factor was found to have no effect on Malaysian participants with only a small impact on Saudi participants. The t-test showed that there was a small difference between Saudi

males and females. The age factor was found, using an ANOVA test, to have no effect on either Saudi or Malaysian participants.

Concerning cultural effects, the regression test proved that religious belief, social norms and Internet regulation affected IT-2 in Saudi Arabia and religious belief, social norms and Internet regulation affected IT-2 in Malaysia. Despite the fact that online trust (as has been mentioned in section 2.3.3) can be affected by the belief that the user's personal information will be kept safe (Dinev and Hart, 2006, p.66), IT skills, in this research, appear to have no effect on Internet trust in Saudi and Malaysia.

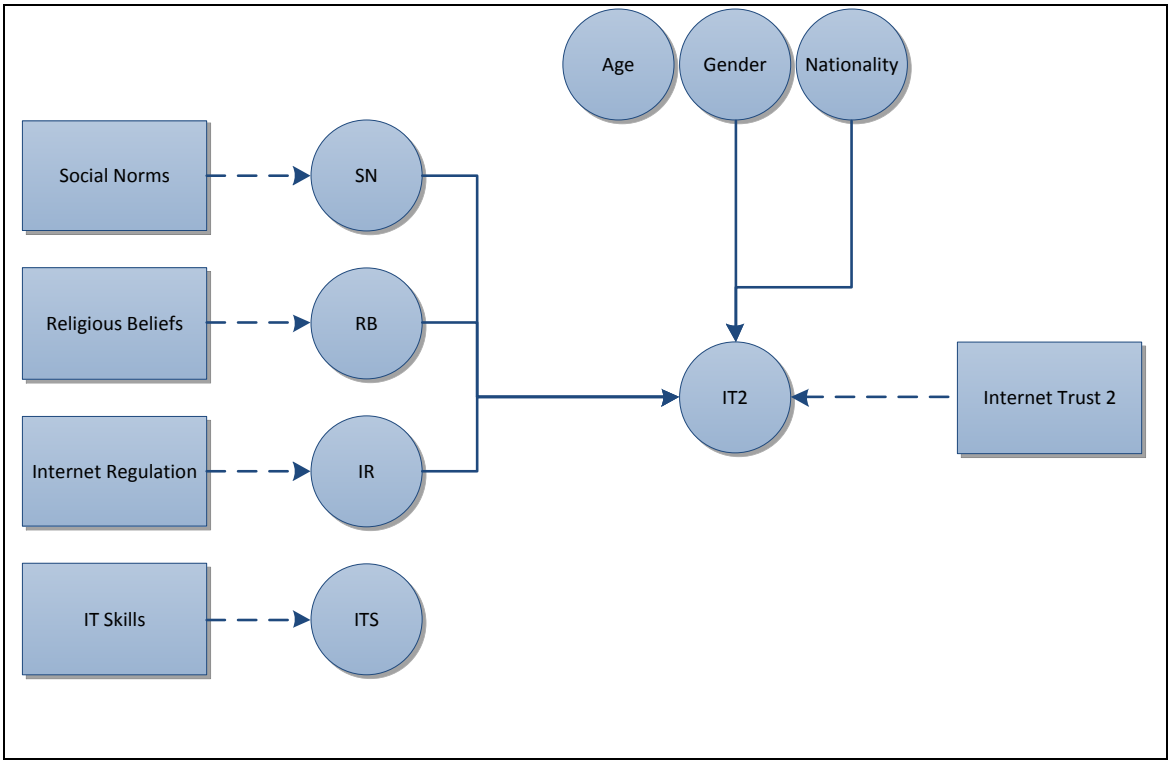


Figure 8-12: The effect of Saudi nationality, gender, age and cultural backgrounds including religious belief, social norms, Internet regulation and IT skills with regards to their trust in the safe online personal Information exchange IT-2

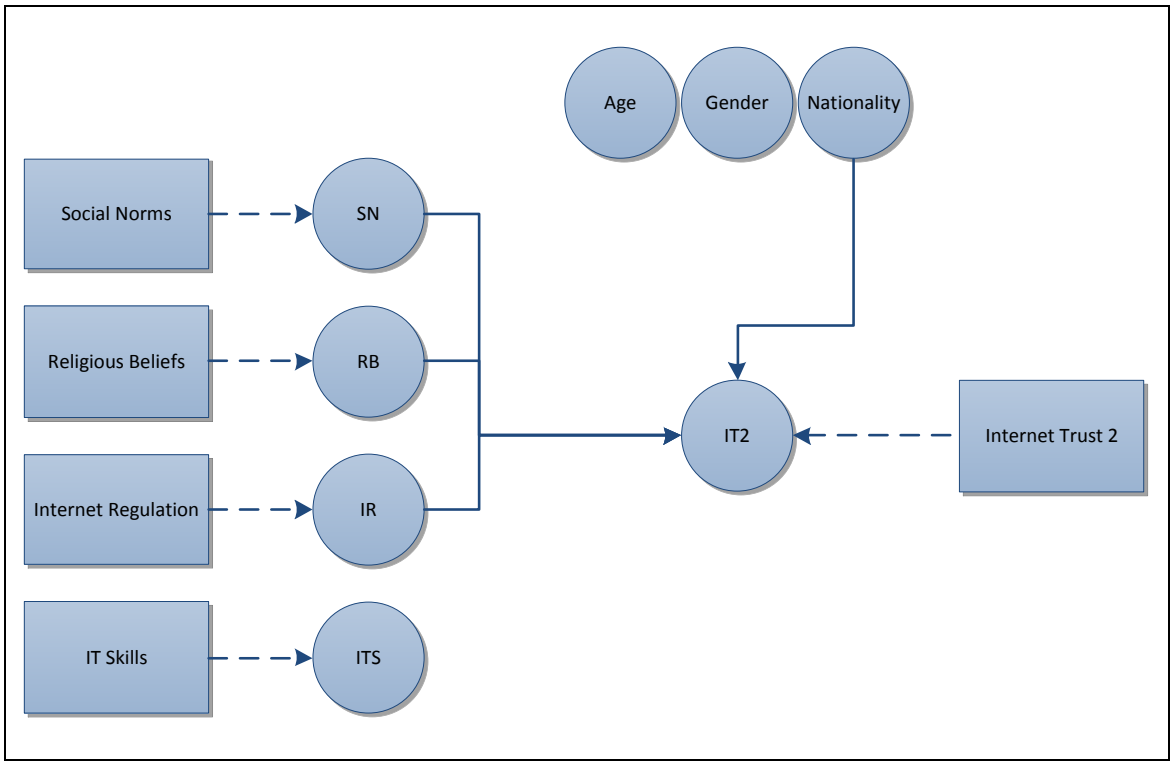


Figure 8-13: The effect of Malaysian nationality, gender, age and cultural backgrounds including religious belief, social norms, Internet regulation and IT skills with regards to their trust in the safety online personal Information exchange IT-2

As mentioned above, the Malaysian participants are more likely to be concerned compared to Saudi participants when they submit personal information via e-mails and Instant Messaging websites. The former also tended to trust the professionalism of e-mail and Instant Messaging services to handle their personal information safely, considering them secure environments in which to exchange personal information more than the Saudis did.

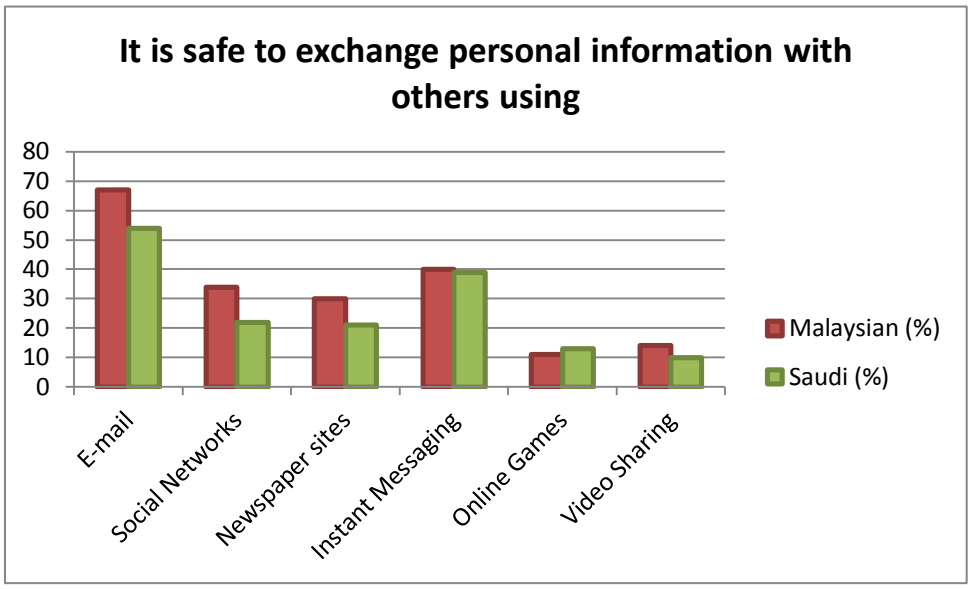


Figure 8-14: Comparison of Malaysian and Saudi participants with regards to their trust in the safe online personal information exchange

8.2.6 SUMMARY OF THE EFFECTS OF NATIONALITY, GENDER AND AGE ON THE PRIVACY PERSPECTIVE

- Malaysian participants tended to consider name, e-mail address, date of birth, nationality and religion as personal information more than Saudis did. In addition, Malaysian participants considered submitting the abovementioned personal information via e-mails, Instant Messaging and Search Engine websites to be a privacy concern. Compared with the Saudi participants, however, they tended to trust the professional handling of their personal information and the security of exchanging this information via the above services;

- Furthermore, Malaysian participants were more likely to be motivated by their family, friends and Internet regulation in Malaysia when looking after their personal information and that of others online;

- With respect to gender differences in Malaysian participants, there is very little in terms of what constitutes personal information. Home address and phone numbers, however, are considered personal information from the male participants' points of view but this is not the case for females;

- Regarding the age factor, for Malaysian participants, it tended to play a role in decreasing the effect of religious beliefs, family and friends on their views upon the importance of guarding and caring for their personal information;

- Saudi participants, on other hand, tended to consider home address, phone number, photographic image and credit card number as personal information more than Malaysian participants did; however, their level of privacy concerns and online trust was lower than that of the Malaysian participants;

- In addition, the Saudi participants' attitudes regarding the guarding of their personal information was driven by their religious beliefs more than was the case for Malaysian participants;
- With regard to the role of gender, female Saudi participants considered home address and photographic image to be personal information compared to their male counterparts. Both female and male participants in Saudi Arabia had the same level of privacy concerns. Male participants, however, were more likely to trust the professional handling of their information and the security of exchanging this information by e-mail, online games, video sharing and live TV websites than their female peers. In addition, male participants tended to be

affected more by their family, friends, Internet regulation and their IT skills in their views about guarding their personal information whereas female participants were more affected by their religious beliefs in their views about the importance of caring for their personal information;

- Regarding the influence of the age factor on the Saudi participants' perspectives, older Saudi participants were more likely than compared to younger ones to consider their first and full name and date of birth as personal information;

- In addition, older Saudi participants were more concerned about submitting personal information via e-mails and websites and had more privacy concerns with regard to submitting personal information using Social Network websites but they trusted e-commerce websites to handle their personal information professionally.

8.3 CULTURAL EFFECTS

The effect of the nationality, gender and age on the cultural backgrounds of the participants including the religious belief (RB), social norms (SN), Internet regulation (IR) and IT skills (ITS) were reported in Chapter 7. A summary discussion of the effect of these factors on cultural backgrounds follows.

8.3.1 RELIGIOUS BELIEFS (RB)

The finding shows that the religious beliefs (RB) are not affected by the nationality factor (see section 7.4.8). The gender factor had no effect either on Malaysian participants and only a small one on the Saudis. The age factor was found to have a

small effect on the Saudi participants and no effect on the Malaysians (Figures 8.15 and 8.16). These results suggest that participants from both Malaysia and Saudi Arabia have the same perception of religious belief in the attitude of online privacy, however as could be seen from sections 8.2.1 – 8.2.6 these effects of religion are not related to privacy concerns and Internet trust with the Malaysian participants.

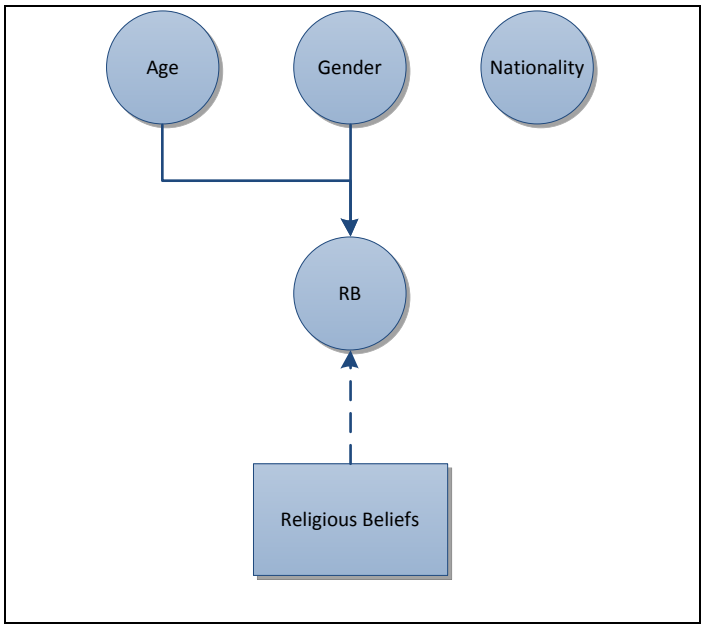


Figure 8-15: The effect of Saudi nationality, gender and age on the religious belief factor

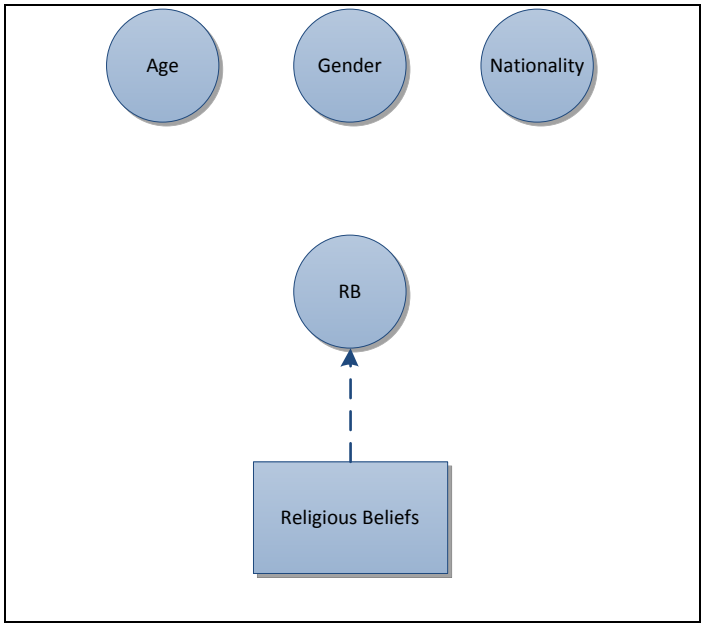


Figure 8-16: The effect of Malaysian nationality, gender and age on the religious belief factor

8.3.2 SOCIAL NORMS (SN)

Social norms (SN) affected the nationality factor. The t-test showed that there was a large difference between Saudi and Malaysian participants. The gender factor was found to have no effect on either Malaysian or Saudi participants. The age factor was found to have no effect on either Malaysian or Saudi participants (Figures 8.17 and 8.18). These results indicate that although participants from Malaysia and Saudi Arabia have different perceptions of the role of social norms on the attitude of online privacy, (as could be seen from sections 8.2.1 to 8.2.6) these effects are not related to privacy concerns and Internet trust in the Saudi cases.

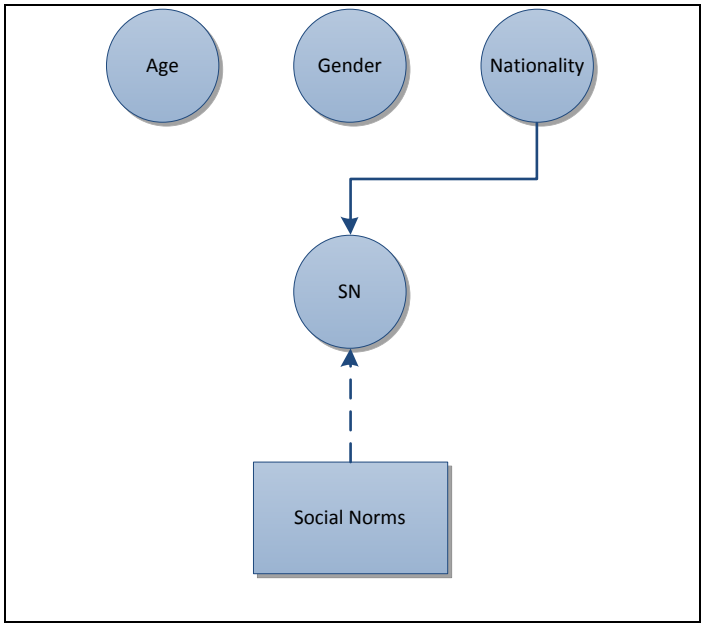


Figure 8-17: The effect of Saudi nationality, gender and age on the social norms factor

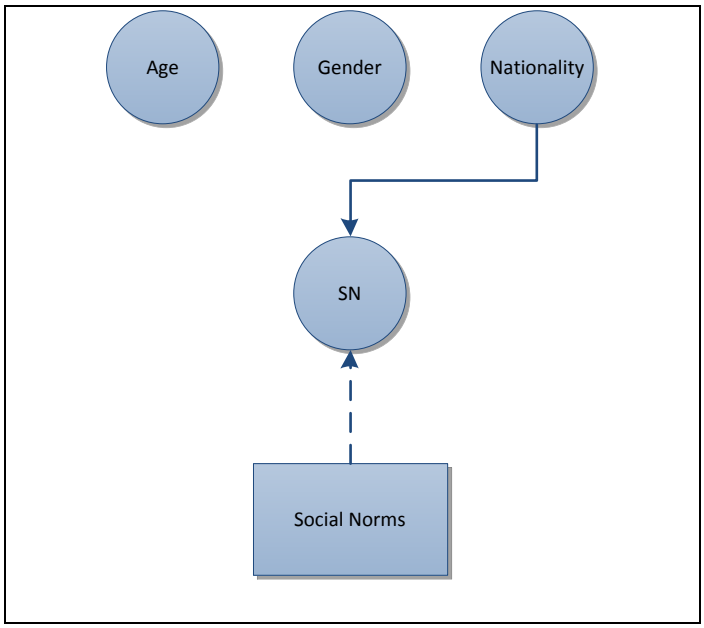


Figure 8-18: The effect of Malaysian nationality, gender and age on the social norms factor

8.3.3 INTERNET REGULATION (IR)

The Internet regulation (IR) appeared to be affected by the nationality factor. The t-test showed that there was a small difference between Saudi and Malaysian participants. The gender factor had no effect on either the Malaysian or the Saudi participants. The age factor was found to have a small effect on the Malaysian participants and no effect on the Saudis (Figures 8.19 and 8.20). These results suggest that participants from both Malaysia and Saudi Arabia have different perceptions of the role of Internet regulation on the attitudes of online privacy, and as could be seen from sections 8.2.1 – 8.2.6 the effects of Internet regulation are not related to privacy concerns and Internet trust in the Saudi cases. This could be because although Saudis appreciate the effect of such Internet regulation, due to the lack of such regulation they do not believe that it works for them. Further investigation is needed to clarify why Saudi's do not consider Internet regulation as a factor in forming their perception of privacy concerns and Internet trust.

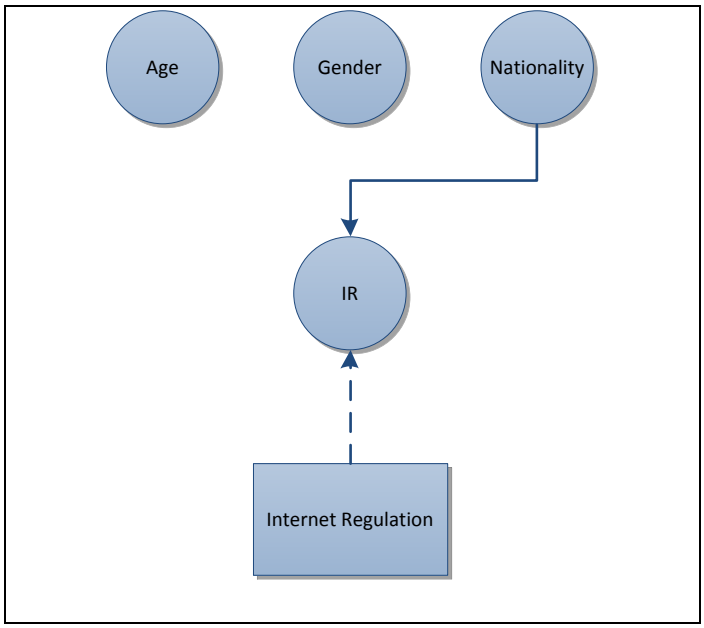


Figure 8-19: The effect of the Saudi nationality, gender and age on the Internet regulation factor

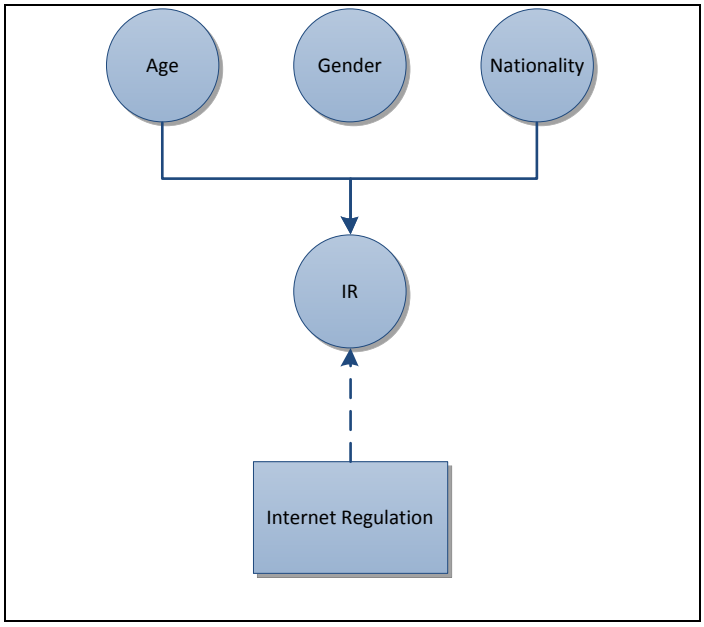


Figure 8-20: The effect of the Malaysian nationality, gender and age on the Internet regulation factor

8.3.4 THE IT SKILL (ITS)

IT skills (ITS) affected the nationality factor. The t-test showed that there was a small difference between Saudi and Malaysian participants. The gender and age factors did not affect either Malaysian or Saudi participants (Figures 8.21 and 8.22). These results

suggest that while participants from Malaysia and Saudi Arabia have different perceptions of the role of IT skills on the attitude of online privacy (as could be seen from sections 8.2.1 to 8.2.6) the effects of social norms are related to privacy concerns and Internet trust (except for IT-2) in both the Malaysian and Saudi cases.

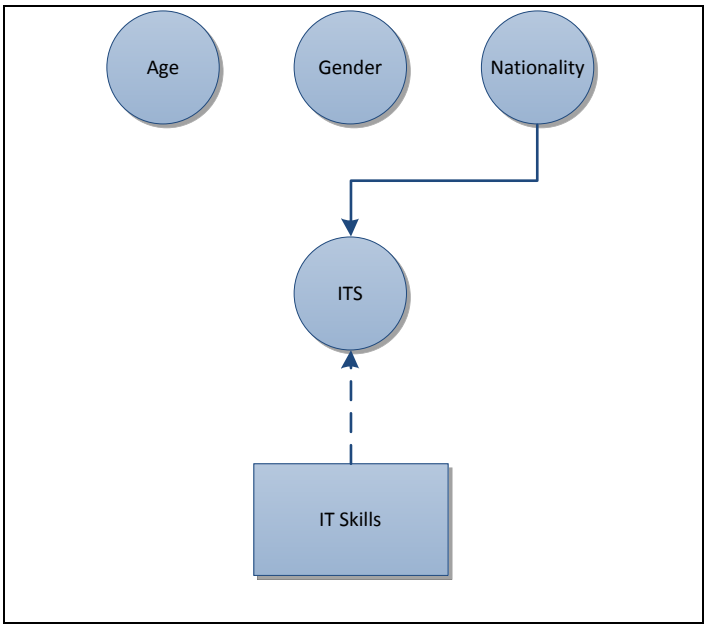


Figure 8-21: The effect of the Saudi nationality, gender and age on the IT skills factor

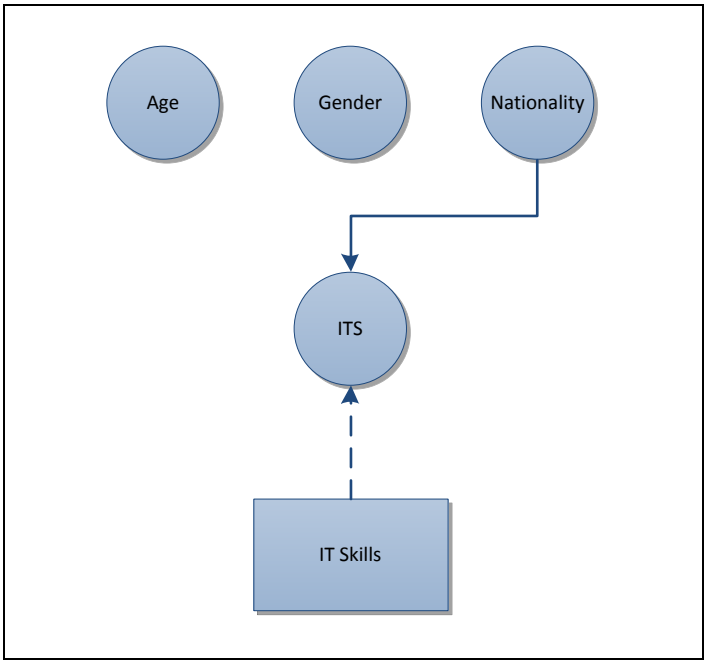


Figure 8-22: The effect of the Malaysian nationality, gender and age on the IT skills factor

8.4 THE RESEARCH HYPOTHESES

A number of hypotheses were proposed in Chapter 5 and the results of testing these hypotheses were reported in Chapter 7. Hypotheses 1 to 4 were designed to address the first research question: Is there a relationship between the level of an individual's Internet privacy concerns and the effects of religious beliefs, IT skills, social norms and local Internet regulation on their online privacy attitudes? Hypotheses 5 to 8 were designed to answer the second research question: Is there a relationship between the level of an individual's Internet trust and the effects of religious beliefs, IT skills, social norms and local Internet regulation on their online privacy attitudes? Hypotheses 9 to 16 were designed to answer the third research question: How well do religious beliefs, IT skills, social norms and local Internet regulation and their effects on individuals predict their Internet privacy concerns and their Internet Trust? Finally, hypotheses 17 to 20 were designed to answer the fourth research question: What are the similarities and differences between individual Muslims with different cultural backgrounds with regards to the effects of religious beliefs, IT skills, social norms and local Internet regulation on both their Internet privacy concerns and their Internet trust?

Before summarising the relationship between Internet users' privacy perspectives and the four cultural effects on online privacy attitudes, as well as nationality, age and gender, it is worth restating the components of the privacy perspective, the proposed cultural effects and the demographic factors that have already been mentioned in Chapter 5.

1. The privacy perspective consists of five components:
    - What is considered to be personal information (P1),

- Privacy concerns about submitting personal information via the Internet (PC)
- Concerns about unauthorized use of the personal information submitted (PC-2)
- Trust with regard to the professional handling of the personal information via the Internet (IT)
- Trust in the safe exchange of the personal information via the Internet (IT-2)

2. Cultural effects on online privacy attitudes consist of four components:

    - Religious beliefs (RB),
    - Social norms (SN),
    - Internet regulation (IR)
    - IT skills (ITS)

3. Demographic Factors consist of three components:

    - Nationality
    - Age
    - Gender

The outcomes stated in Chapter 6 and 7 were the results of two statistical tests. First, is the contingency analysis for the relationship between privacy concerns, Internet trust and the three demographic factors, that is, nationality, age and gender. Second, the simple regression analysis to test the proposed hypotheses, that is, examining the relationship between privacy concerns (PC, PC-2) and Internet trust (IT and IT-2) and the four cultural effects (RB, SN, IR and ITS). The outcomes of these tests helped in developing the research model that was suggested in Chapter 5 (see Figure 8.23).

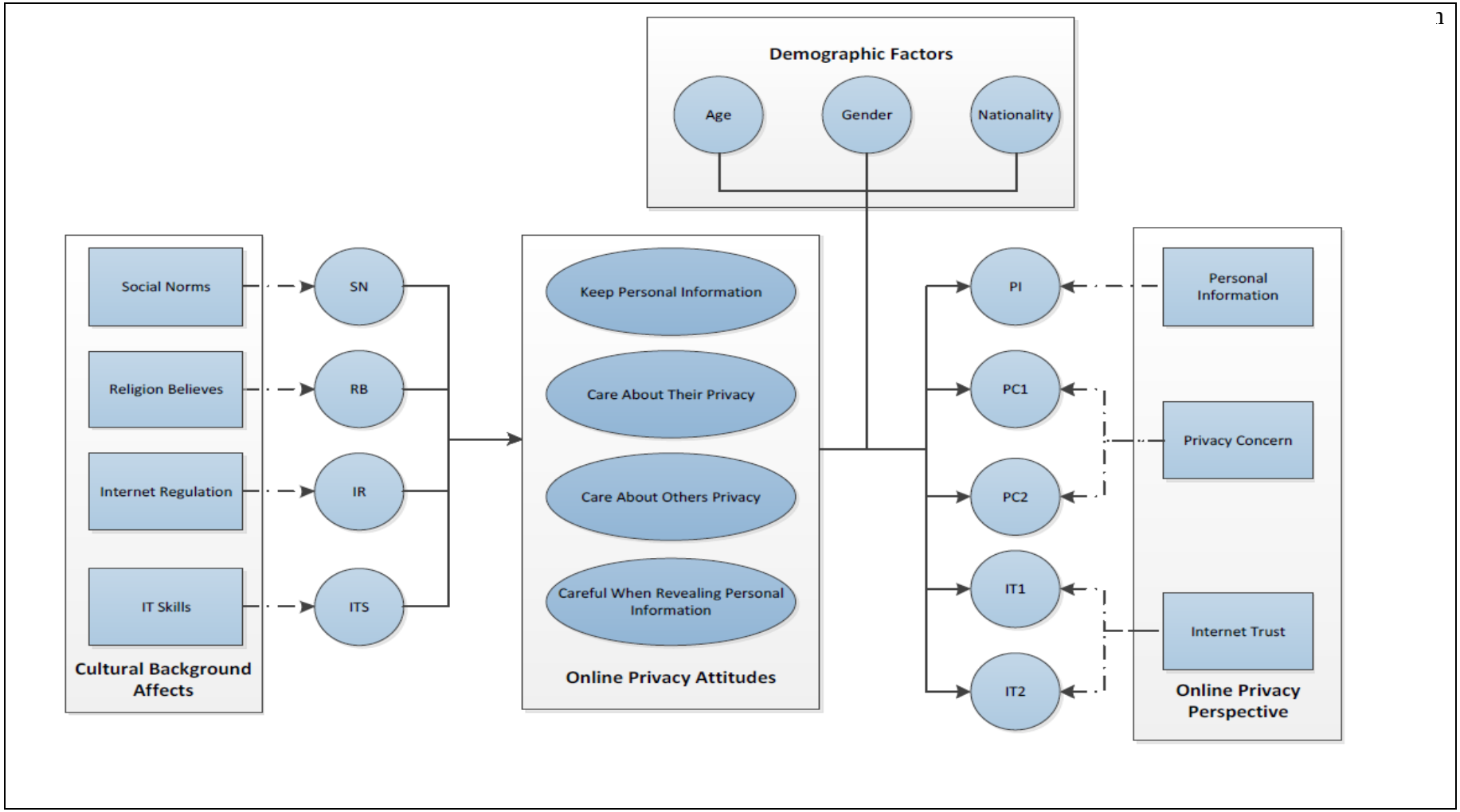


Figure 8-23: Proposed model of the effect of cultural background, nationality, age and gender on the privacy perspective

There now follows a detailed review of each relationship within the research model by country.

8.4.1 MALAYSIA

Firstly, social norms, Internet regulation and IT skills but not religious beliefs could be related to privacy concerns about submitting personal information via the Internet (PC-1) (Figure 8.24) and the unauthorized use of this data (PC-2) (Figure 8.25).

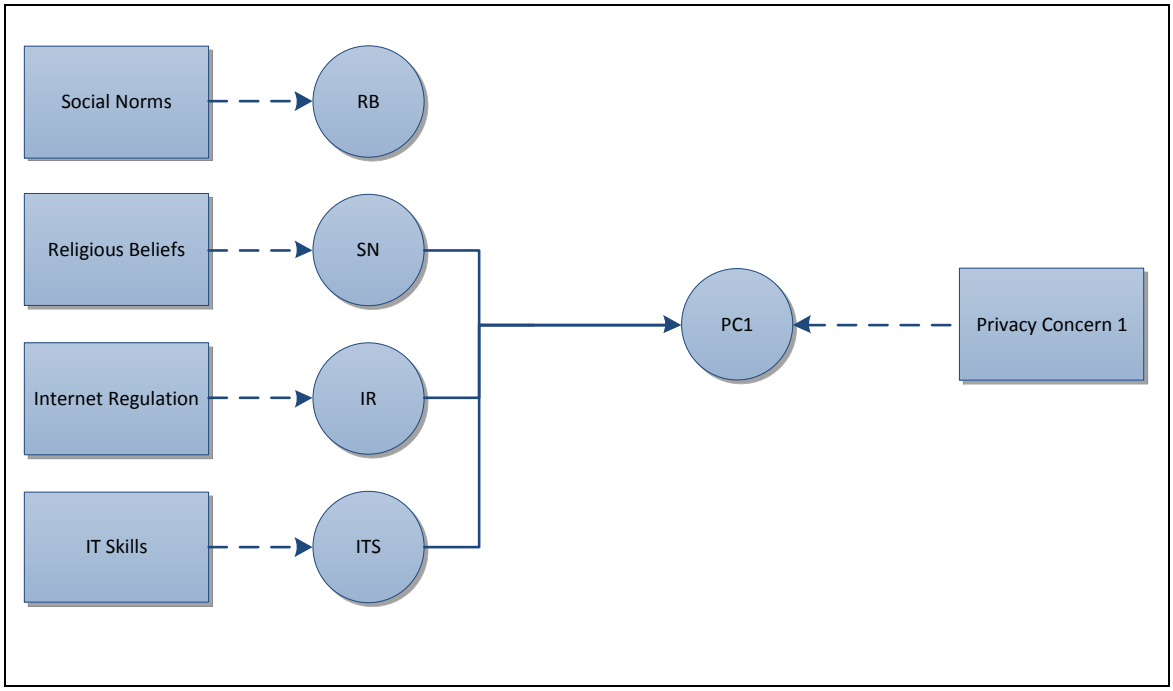


Figure 8-24: Outcomes model for the effect of the cultural background on privacy concerns about submitting personal information via the Internet (PC-1) in Malaysia

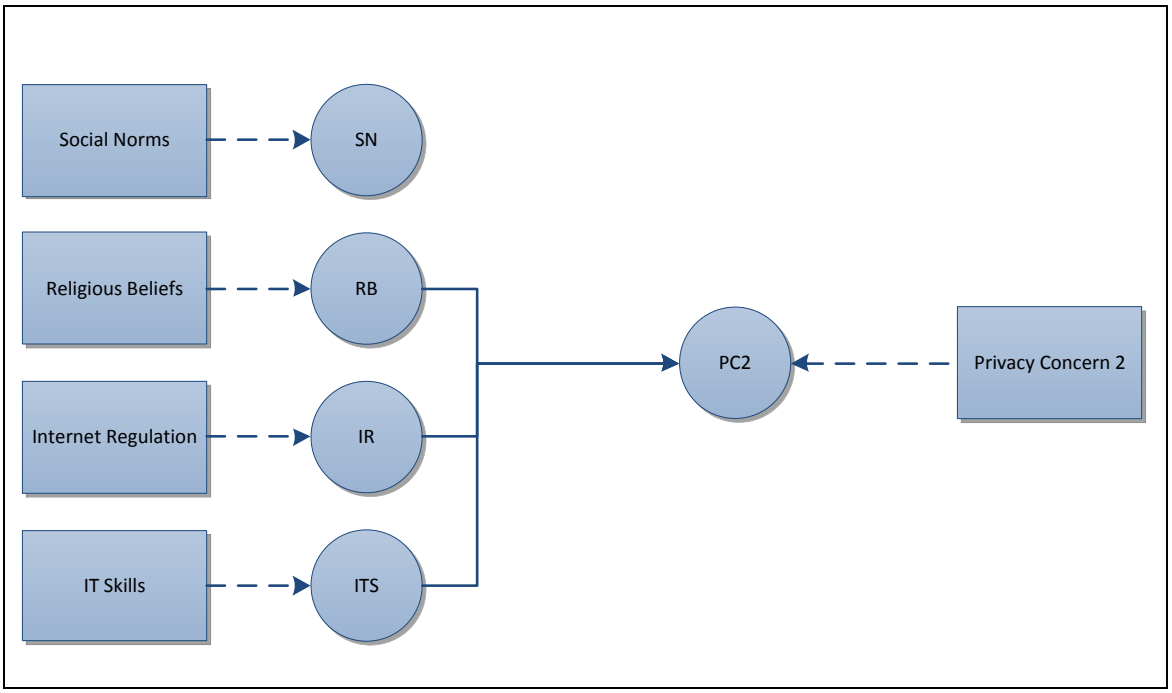


Figure 8-25: Outcomes model for the effect of the cultural background on privacy concerns about the unauthorized use of this data (PC-2) in Malaysia

Secondly, only nationality could be related to privacy concerns about submitting personal information via the Internet (PC-1) (Figure 8.26) whereas nationality and age factors were related to concerns about the unauthorized use of personal information (PC-2) (Figure 8.27).

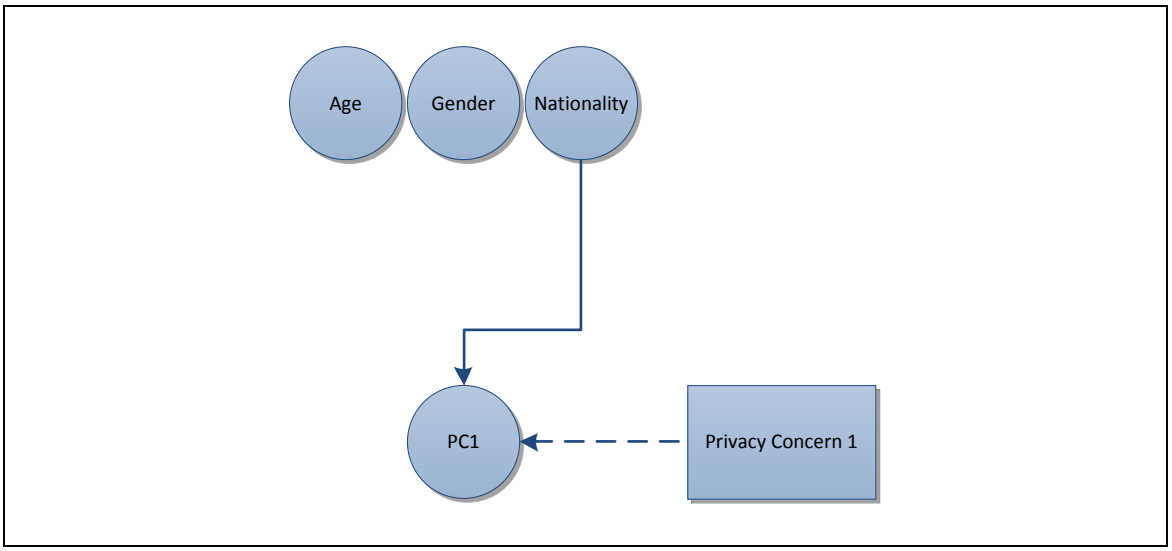


Figure 8-26: Outcomes model for the effect of nationality, gender and age on privacy concerns about submitting personal information via the Internet (PC-1) in Malaysia

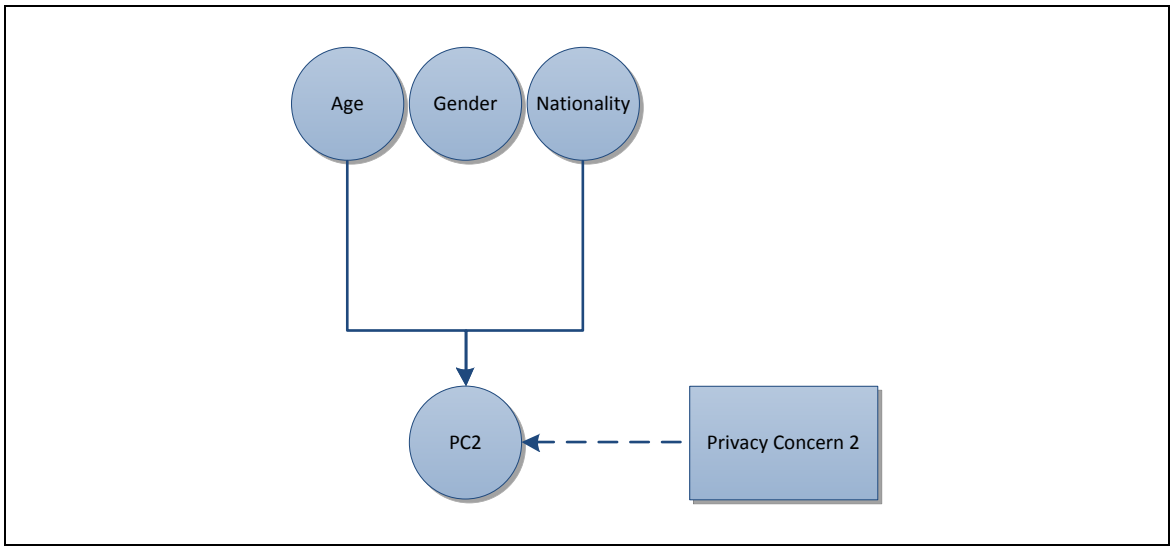


Figure 8-27: Outcomes model for the effect of nationality, gender and age on privacy concerns about the unauthorized use of this data (PC-2) in Malaysia

Thirdly, religious belief, IT skills, social norms and Internet regulation could be related to Internet trust with regard to the professional handling of personal information via the Internet (IT-1) (Figure 8.28) whereas only social norms and Internet regulation could be related to trust in its safe exchange (IT-2) (Figure 8.29).

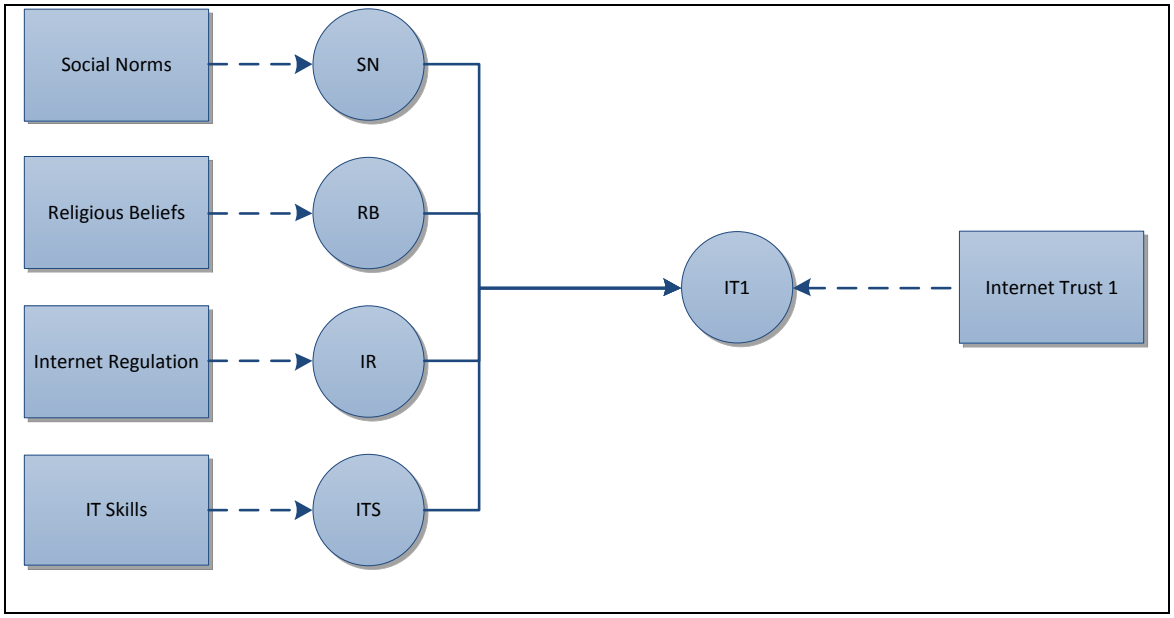


Figure 8-28: Outcomes model for the effect of the cultural background on Internet trust in Malaysia

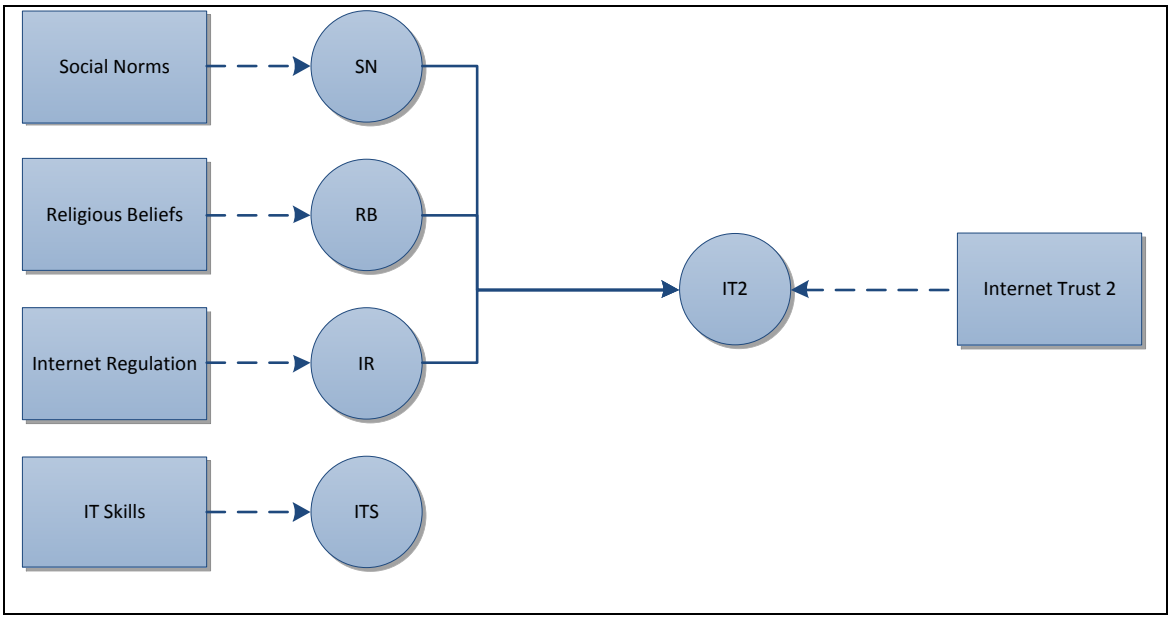


Figure 8-29: Outcomes model for the effect of the cultural background on Internet trust in Malaysia

Furthermore, only nationality could be related to Internet trust with regard to both the professional handling of personal information via the Internet (IT-1) (Figure 8.30) and its safe exchange (IT-2), (Figure 8.31).

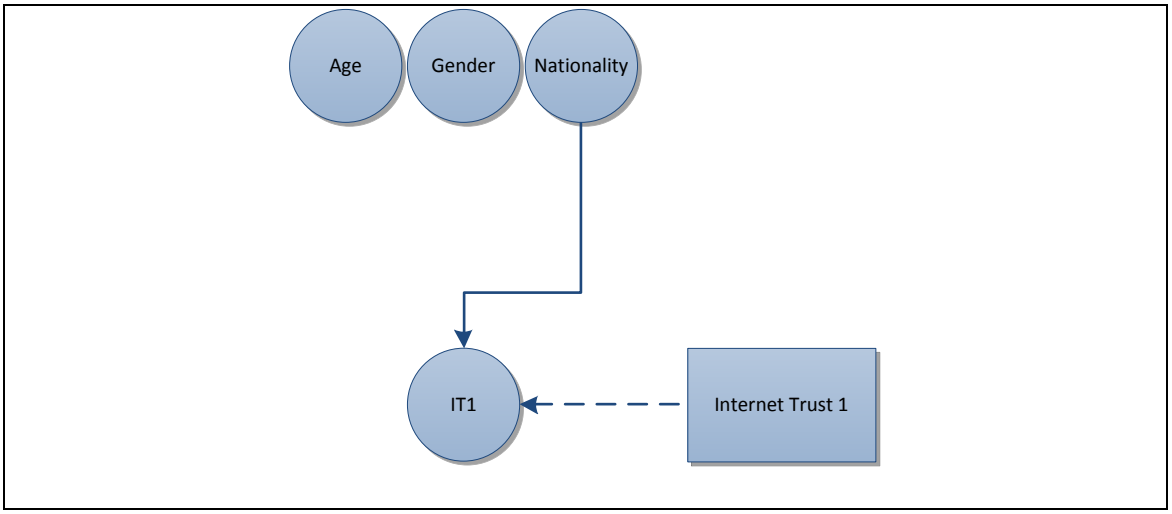


Figure 8-30: Outcomes model for the effect of the nationality, gender and age on Internet trust in professional handling of personal information via the Internet (IT-1) in Malaysia

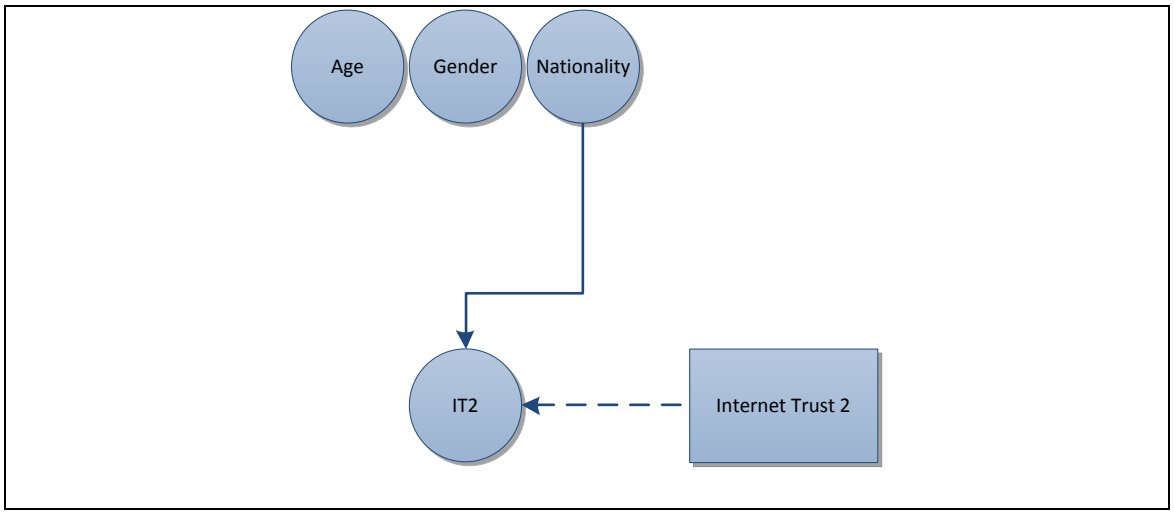


Figure 8-31: Outcomes model for the effect of the nationality, gender and age on Internet trust on its safe exchange (IT-2) in Malaysia

8.4.2 SAUDI ARABIA

Firstly, the effect of religious belief, IT skills, social norms and Internet regulation are related to privacy concerns about submitting personal information via the Internet (PC-1) (Figure 8.32) whereas only religious belief and IT skills have been shown to be related to concerns about unauthorized use of the personal information that is submitted (PC-2) (Figure 8.32).

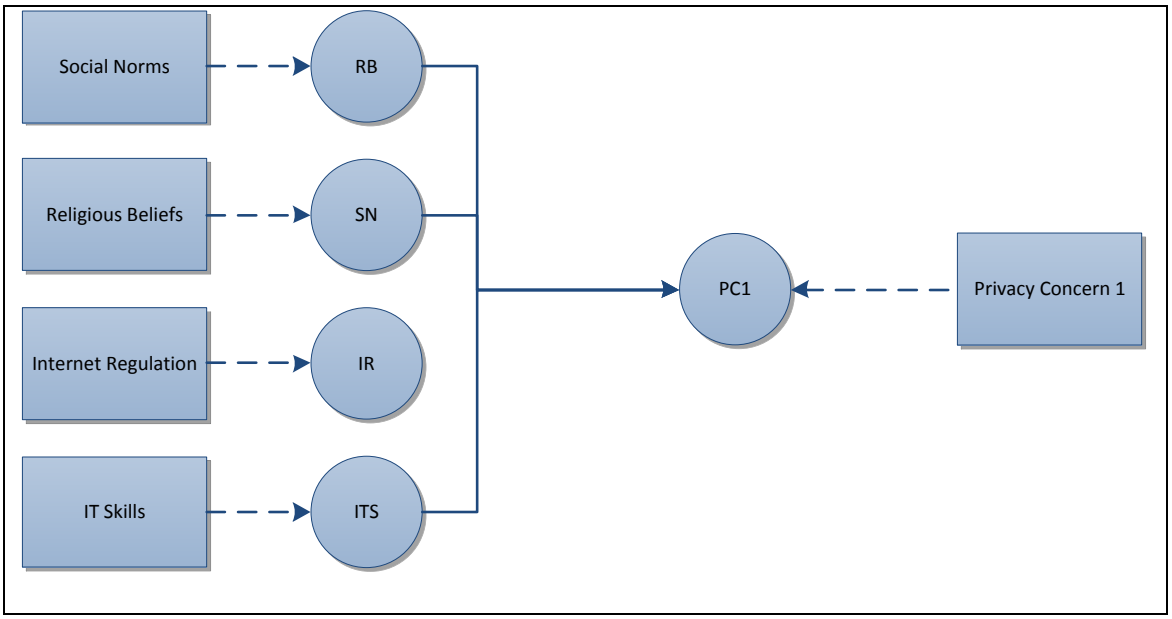


Figure 8-32: Outcomes model for the effect of the cultural background on privacy concerns about submitting personal information via the Internet (PC-1) in Saudi Arabia

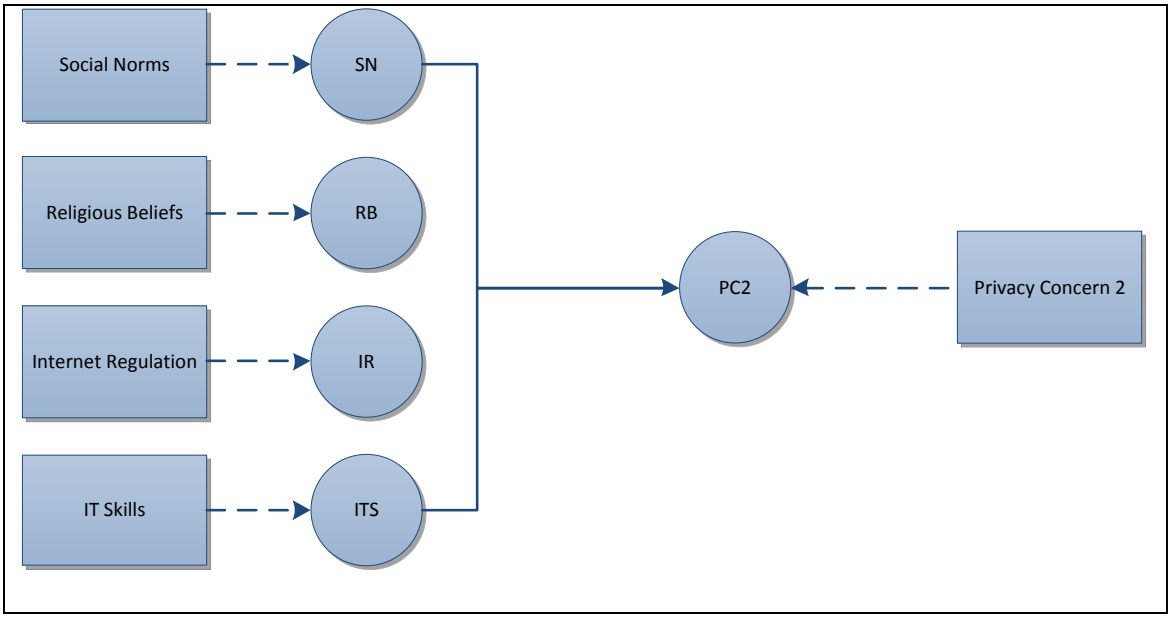


Figure 8-33: Outcomes model for the effect of the cultural background on privacy concerns about unauthorized use of the personal information that is submitted (PC-2) in Saudi Arabia

Secondly, nationality and age are related to privacy concerns about submitting personal information via the Internet (PC-1) (Figure 8.34) whereas nationality and gender are related to concerns about its unauthorized use (PC-2), (Figure 8.34). The effect of

gender on privacy perception, particularly concerns about the unauthorized use of online personal information, could be due to women, unlike men, feeling that they do not have the desirable level of privacy and face privacy problems that arise from their perception of being subordinate and easy targets (Allen, 2000, p.1178) and therefore, instead, women claim more protection for their private conduct and information. Such acts show a replication of the real world's complex gendered social norms of accessibility and inaccessibility in the cyber world (Allen, 2000, p.1178). These gender differences were not the case in Malaysia, which suggests that women might do not experience the same gender norms online. Further research might reveal an interesting explanation of these differences in the gender factor between Malaysians and Saudis.

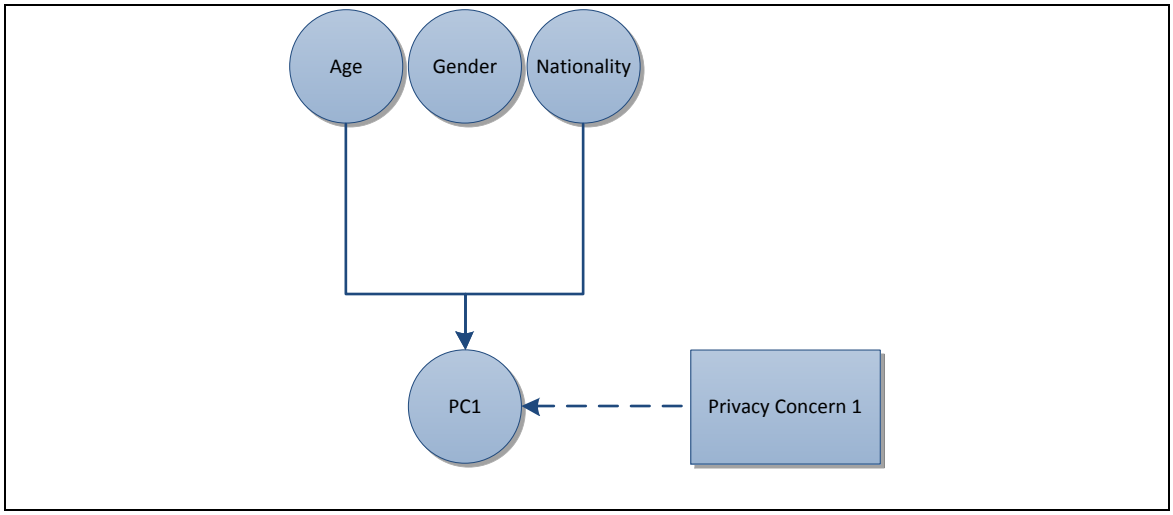


Figure 8-34: Outcomes model for the effect of nationality, gender and age on privacy concerns about submitting personal information via the Internet (PC-1) in Saudi Arabia

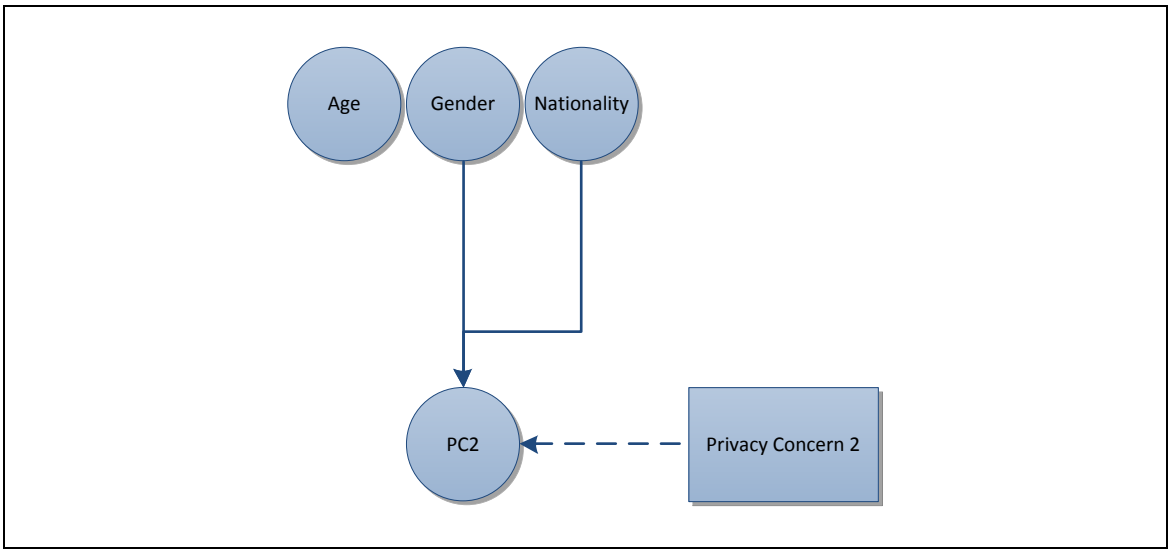


Figure 8-35: Outcomes model for the effect of nationality, gender and age on privacy concerns about unauthorized use of the personal information that is submitted (PC-2) in Saudi Arabia

Thirdly, all religious beliefs, social norms, Internet regulation and IT skills are related to Internet trust with regard to the professional handling of personal information via the Internet (IT-1) (Figure 8.36) whereas religious beliefs, social norms and Internet regulation are related to trust in its safe exchange (IT-2), (Figure 8.37).

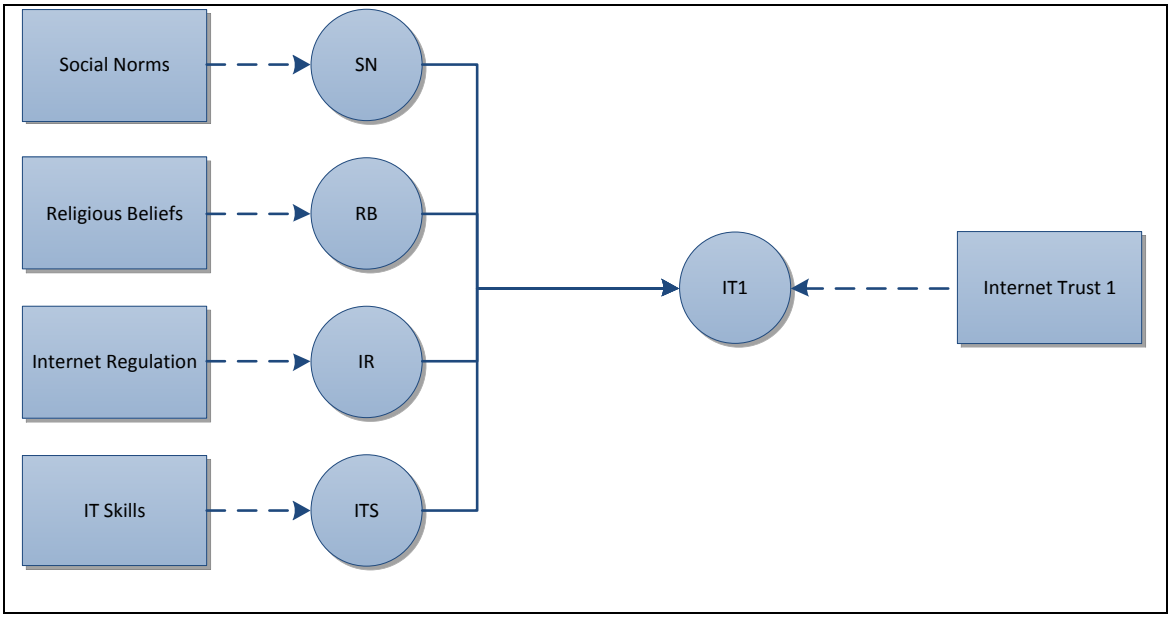


Figure 8-36: Outcomes model for the effect of the cultural background on Internet trust in the professional handling of personal information via the Internet (IT-1) in Saudi Arabia

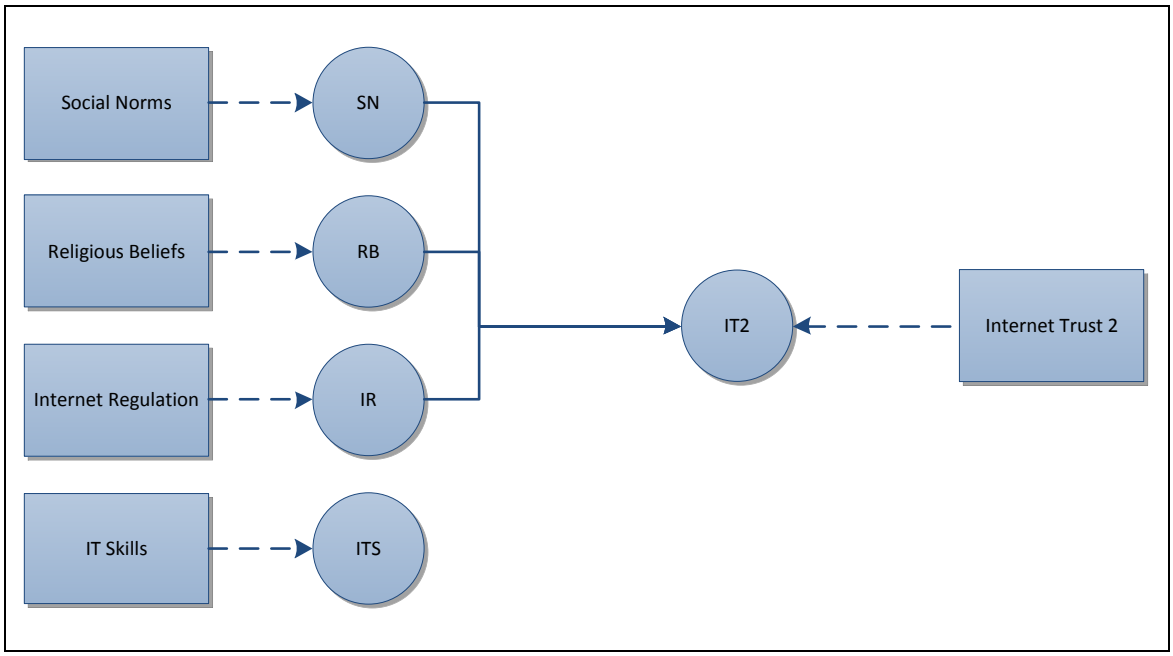


Figure 8-37: Outcomes model for the effect of the cultural background on Internet trust in its safe exchange (IT-2) in Saudi Arabia

Fourthly, only nationality is related to Internet trust with regard to the professional handling of personal information via the Internet (IT-1) (Figure 8.38) whereas nationality and gender could be related to its safe exchange (IT-2) (Figure 8.39). As mentioned above, the gender differences could be due to a replication of the real world's complex gendered social norms of accessibility and inaccessibility in the cyber world (Allen, 2000, p.1178) in Saudi Arabia.

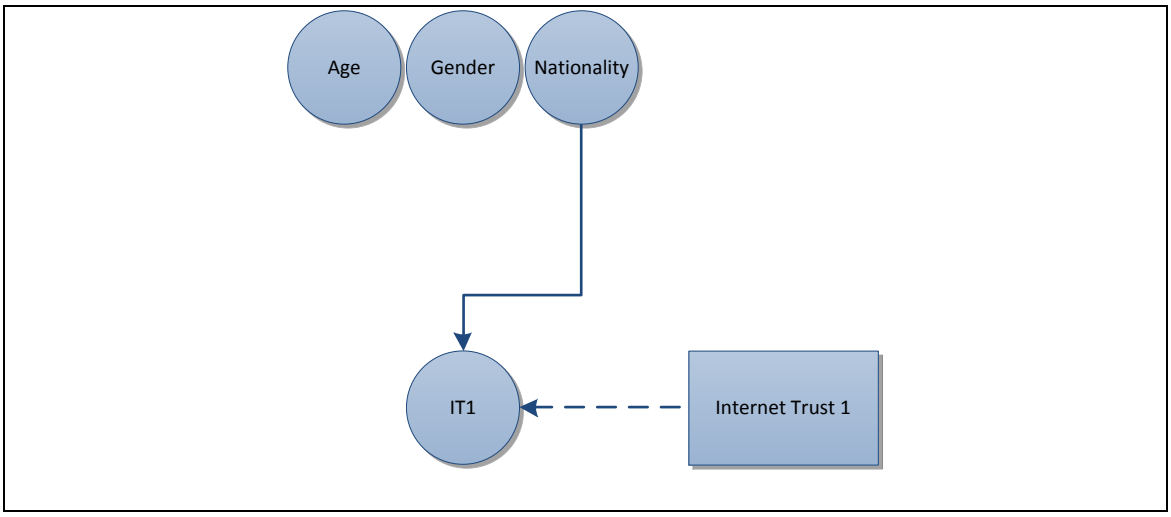


Figure 8-38: Outcomes model for the effect of the nationality, gender and age on Internet trust in the professional handling of personal information via the Internet (IT-1) in Saudi Arabia

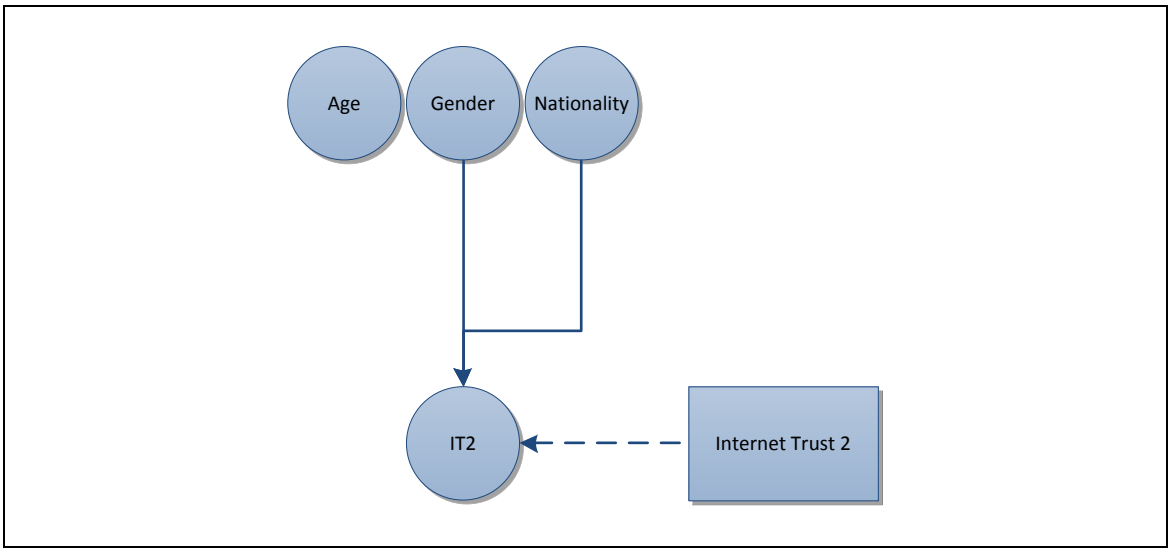


Figure 8-39: Outcomes model for the effect of the nationality, gender and age on Internet trust in its safe exchange (IT-2) in Saudi Arabia

8.5 CONCLUSION

In this chapter, the effects of nationality, gender and age factors on online privacy concerns and trust and online privacy attitude were discussed in the light of the literature review. For example, according to Guarda and Zannone's classification of personal information (2008, p.7), Malaysian students consider personal data (name, e-mail address and date of birth) and sensitive data (nationality and religion) as personal

information whereas Saudi participants consider personal data (home address, phone number and photographic image) and credit card number.

In this chapter the comparison between Malaysian and Saudi participants in terms of their perceptions of online privacy concerns and Internet trust, as well as the differences of the effects of the cultural (religious beliefs, social norms, Internet regulation and IT skills) and demographic (age, gender and nationality) factors on online privacy attitude were demonstrated.

Furthermore this chapter summarized the cultural influences that affect the privacy perspectives of individual Saudi and Malaysian Muslims in their internet usage while at the same time identifying the similarities and differences between these perspectives. Finally, outcomes derived from the research hypothesis for both Malaysian and Saudi Internet users, which includes the model for the relation between the privacy perspectives and demographic and cultural effects were discussed.

9 CHAPTER 9: CONCLUSION AND RECOMMENDATION

9.1 RESEARCH SUMMARY

The purpose of this study has been to investigate the relationship between people's online privacy perspectives and their cultural background, in particular religious beliefs, IT skills, social norms and Internet regulations, as well as the age, gender and nationality of Internet users. To achieve this purpose two main aims were formulated. The first aim was to identify cultural influences that affect the privacy perspectives of individual Muslims from Saudi Arabia and Malaysia when they use the Internet. The second aim was to identify the similarities and differences between the perspectives of Saudi Arabian and Malaysian participants on the issue of privacy in Internet usage.

In order to fulfil the research requirements, the research strategy began with a number of focus groups to build up a general picture of what constitutes personal information from the participants' points of view, the nature of their online privacy perspectives and what factors might affect these perspectives. Then, in accordance with the research strategy, the main data collection tool (the questionnaire) was designed, subsequently tested and piloted. This was followed by a data collection and analysis phase.

Data was initially collected to establish what information was considered 'personal' according to Malaysian and Saudi participants. The results showed that there was a difference between Malaysian and Saudi participants. The Malaysian participants considered name, e-mail address, and date of birth, their nationality and religion to be personal; males, unlike females, considered the home address and phone numbers as 'personal' information. The Saudi participants were more likely to consider home

address, phone number, photographic image and credit card number as personal information. Gender plays a role in the Saudi cases too, as the Saudi female considers home address and photographic image to be 'personal' information compared to the male.

Next, the level of privacy concerns when submitting personal information was reported from the Malaysian and Saudi points of view. The results showed that one-third to a half of the Malaysian participants experienced concerns about submitting their personal information via a Search Engine or Newspaper website. Their level of concern was raised when interacting with communication websites (e-mail, Instant Messaging and Social Networks). Here, two-thirds of the Malaysian participants expressed their reservations. One-third of the Malaysian participants expressed concern about submitting their personal information via entertainment sites (Online Games, Video Sharing websites and Live TV). Of Saudi participants, one-third expressed their concern about submitting their personal information via Search Engines and through Newspaper, communication and entertainment websites while about half of the Saudi participants were concerned about submitting their personal information to business websites (e-Commerce, Online Banking and e-Government).

In addition, more than two-thirds of the Malaysian participants believe that it is safe to exchange their personal information via e-mail whereas only one-third or less share the same belief with regard to Social Networks, Instant Messaging, Newspaper sites, Online Games and Video Sharing. Similarly, in Saudi Arabia, while more than half the participants consider e-mail to be a safe environment for the exchange of personal information, only one-third or less believe that sharing such information is secure via

Instant Messaging, Social Networks, Newspaper sites, Online Games and Video Sharing. Saudi males are more likely to trust the professional handling of their information and the security of exchanging this information by e-mail, online games, video sharing and live TV websites than compare to the Saudi females.

The level of Malaysian concerns and trust with regard to submitting personal information via the Internet was related mostly to the degree to which their social norms affected their online privacy attitudes while other cultural effects, particularly the effect of Internet regulation and IT skills on online privacy attitudes had a lower impact.

Regarding the Saudi participants, the level of their concerns and trust with regard to submitting personal information via the Internet were related mostly to the impact of their IT skills upon their online privacy attitudes while other cultural effects, particularly the effect of their religious beliefs, social norms and Internet regulation had less impact on their online privacy attitudes.

Finally, social norms seemed to have a greater cultural effect upon Malaysian internet users compared to Saudis whose privacy perspectives were affected more by their religious beliefs. Furthermore, Internet regulation in each country and the IT skills of the participants tended to have an equal effect on the privacy perspectives of the participants in both countries.

9.2 ANSWERING THE RESEARCH QUESTIONS

The previous section summarized the research's results. In this section, its findings will be applied to answer the research questions that were formulated to address the aims of this inquiry.

In order to answer the four research questions twenty hypotheses were formulated, which were subsequently tested using Simple Linear Regression analysis.

9.2.1 FIRST RESEARCH QUESTION

With regard to the first research question, which was: ***Is there a relationship between the level of concerns over Internet privacy and the effects of an individual's religious beliefs, IT skills, social norms and local Internet regulation on their attitudes to online privacy?*** Four hypotheses were derived and tested for both countries as follows.

> ***Hypothesis 1:*** *A higher level of Internet privacy concerns is related to the higher impact of an individual's religious beliefs on their online privacy attitudes.*

Saudi Arabian participants' privacy concerns about submitting personal information via the Internet and its possible misuse might be affected by their religious beliefs but there is no evidence for this with respect to the Malaysians.

> ***Hypothesis 2:*** *A higher level of Internet privacy concerns is related to the higher impact of social norms on individuals' online privacy attitudes*.

Participants' privacy concerns about submitting personal information via the Internet and its possible misuse may be affected by social norms in both Malaysia and Saudi Arabia.

> ***Hypothesis 3:*** *A higher level of Internet privacy concerns is related to a higher impact of the local Internet regulation on individuals' online privacy attitudes.*

Both Malaysian and Saudi participants' privacy concerns about submitting personal information via the Internet may be affected by Internet regulations in their countries. In particular, concerns about the possible misuse of submitted personal information are not significantly associated with the effect of local Internet regulations in either country.

> ***Hypothesis 4:*** *A higher level of Internet privacy concerns is related to the higher impact of individuals' IT skills on their online privacy attitudes.*

Malaysian and Saudi participants' privacy concerns about submitting personal information via the Internet and its possible misuse may be affected by their IT skills.

In summary, the privacy concerns of the Malaysian participants were affected by social norms, IT regulation and IT skills. The first two factors (social norms and IT regulation) affected concerns about submitting personal information via the Internet together with its possible misuse whereas IT skills only affected concerns about submitting personal information via the Internet. Privacy concerns of the Saudi participants' were affected by religious beliefs, social norms, IT regulation and IT skills. The first two factors (social norms and IT regulation) affected concerns about submitting personal information via the Internet together with its possible misuse whereas IT skills only affected concerns about submitting personal information via the Internet.

9.2.2 SECOND RESEARCH QUESTION

With regard to the second research question, which was: ***Is there a relationship between the level of trust in the Internet and the effects of an individual's religious beliefs, IT skills, social norms and local Internet regulation on their attitudes to online privacy?*** Four hypotheses were formed and tested for both countries as follows.

Hypothesis 5: *A higher level of Internet trust is related to the higher impact of individuals' religious beliefs on their online privacy attitudes.*

Malaysian and Saudi participants' trust in the professional handling of their personal information and its safe exchange via the Internet were affected by their religious beliefs.

Hypothesis 6: *A higher level of Internet trust is related to the higher impact of social norms on individuals' online privacy attitudes.*

Malaysian and Saudi participants' trust in the professional handling of their personal information and its safe exchange via the Internet were affected by their social norms.

Hypothesis 7: *A higher level of Internet trust is related to a higher impact of local Internet regulation on individuals' online privacy attitudes.*

Malaysian and Saudi participants' online trust in the professional handling of their personal information via the Internet is affected by the Internet regulations of their respective countries. Only Saudi participants trusted the safe exchange of their personal information via the Internet as their perspective was affected by local Internet regulation.

Hypothesis 8: *A higher level of Internet trust is related to the higher impact of individuals' IT skills on their online privacy attitudes.*

Malaysian and Saudi participants' trust in the professional handling of their personal information via the Internet was affected by their IT skills. Trust in the safe exchange of

their personal information via the Internet in both countries was not statistically associated with the effect of their IT skills, once personal information was submitted.

In summary, trust in the Internet by Malaysian participants was affected by their religious beliefs, social norms, IT regulation and IT skills. The first two factors (religious beliefs and social norms) affected trust in the professional handling of their personal information and its safe exchange via the Internet. The last two factors (IT regulation and IT skills) only affected trust in the professional handling of their personal information via the Internet. Trust in the Internet by Saudi participants was affected by their religious beliefs, social norms, IT regulation and IT skills. The first three (religious beliefs, social norms and IT regulation) affected trust in the professional handling of their personal information and its safe exchange via the Internet. The last factor (IT regulation) only affected trust in the professional handling of their personal information via the Internet.

9.2.3 THIRD RESEARCH QUESTION

With regard to the third research question, which was ***How do religious beliefs, IT skills, social norms and local Internet regulations affect Internet privacy concerns and Internet trust?***

Eight hypotheses were formed and tested for both countries as follows.

> ***Hypothesis 9****: The effect of Internet users' religious beliefs on their Internet privacy concerns is greater than other factors, that is, IT skills, social norms and Internet regulation.*

***Hypothesis 10**: The effect of social norms on Internet users' Internet privacy concerns is greater than the other factors, that is, religious beliefs, IT skills and Internet regulation.*

***Hypothesis 11**: The effect of local Internet regulation on Internet users' Internet privacy concerns is greater than the other factors, that is, religious beliefs, IT skills and social norms.*

***Hypothesis 12**: The effect of Internet users' IT skills on their Internet privacy concerns is greater than the other factors, that is, religious beliefs, social norms, and Internet regulation.*

For the Malaysian participants social norms tended to be the most influential factor associated with participants' privacy concerns with regard to submitting personal information via the Internet for Malaysian users. Religious beliefs seemed to be the most important factor for Saudi participants. Furthermore, local Internet regulation acted as the most influential factor on users' privacy concerns with regard to the possible misuse of their personal information via the Internet in both countries.

***Hypothesis 13**: Internet users' religious beliefs have a greater effect on their Internet trust than other factors, that is, IT skills, social norms and Internet regulation.*

***Hypothesis 14**: Social norms have a greater effect on Internet users' Internet trust than other factors, that is, religious beliefs, IT skills and Internet regulation.*

Hypothesis 15*: Local Internet regulation has a greater effect on Internet user's Internet trust than other factors, that is, religious beliefs, IT skills and social norms.*

Hypothesis 16*: Internet users' IT skills have a greater effect on their Internet trust than other factors, that is, religious beliefs, social norms, and Internet regulation.*

Social norms tended to be the most influential factor associated with Malaysian trust in the professional handling of their personal information via the Internet (as with privacy concerns). Again religious beliefs seem to be the most influential factor from the Saudi point of view. Furthermore, local Internet regulation proved the most influential factor associated with Internet users' trust in the safe exchange of their personal information via the Internet for Malaysians. Religious beliefs seemed to be the most important factor from the Saudi point of view.

9.2.4 FOURTH RESEARCH QUESTION

With regard to the fourth research question, which was ***What are the similarities and differences between individual Muslims from different cultural backgrounds with regard to the effects of religious beliefs, IT skills, social norms and local Internet regulation on both their Internet privacy concerns and their Internet trust?***

Four hypotheses were formed and tested for both countries as follows.

Hypothesis 17: *Religious beliefs have a greater influence on the privacy perspectives of individuals in Malaysia than on those in Saudi Arabia.*

Hypothesis 18: *Social norms have a greater influence on the privacy perspectives of individuals in Malaysia than on those in Saudi Arabia.*

Hypothesis 19: *Internet regulation has a greater influence on the privacy perspectives of individuals in Malaysia than on those in Saudi Arabia.*

Hypothesis 20: *IT skills have a greater influence on the privacy perspectives of individuals in Malaysia than on those in Saudi Arabia.*

Malaysian privacy perspectives tended to be more associated more with the social norms factor compared with the Saudi privacy perspective, which tends to be more associated with the factor of religious beliefs. Moreover, Malaysian and Saudi privacy perspectives have a similar level of association with both local Internet regulation and an individual's IT skills.

9.3 RESEARCH CONTRIBUTIONS

The findings of the research contribute to understanding the impact of cultural background and gender on individuals' perspectives on privacy using the Internet. The study conducted a literature review to arrive at an understanding of different cultural views regarding privacy, particularly with respect to the relationship between online privacy perspectives and cultural background, including religious beliefs, IT skills, social norms and Internet regulation, as well as the nationality and gender of the Internet users. A gap in knowledge was found and as a result the research has been able to develop and validate a quantitative instrument, that is, a questionnaire, which integrates variables to measure the impact of cultural background (in terms of religious beliefs, IT skills, social norms, Internet regulation, nationality and gender) on online privacy

attitudes. It has thus modelled a way of measuring privacy perspectives in order to link these to one or more cultural effects. The outcomes of this quantitative research, which are supported by a literature review and empirical evidence generated through statistical analyses have resulted in the following contributions:

1. The contribution of this study is its provision of understanding of what cultural influences might most affect the privacy perspectives of Internet users in Malaysia and Saudi Arabia. The outcomes suggest that Malaysian privacy perspectives are affected mostly by their social norms whereas Saudi privacy perspectives are affected mainly by their religious beliefs. Other cultural factors, particularly the Internet regulation in force in each country and the IT skills of participants, tend to have an equal effect on both Malaysian and Saudi privacy perspectives. This finding could benefit future IS research into an individual's privacy perspectives, as well as benefiting web designers by prompting them to take these cultural effects into account when designing their websites' privacy policy.
2. This study can add to the existing body of research on Internet privacy perspectives (Chan *et al.*, 2002, p.139; Zakaria *et al.*, 2003, p.57; Ballman *et al.*, 2004, p. 313; Siala *et al.*, 2004, p.7; Dinev *et al.*, 2005, p.2; Xu *et al.*, 2008, p.7). Such inquiries investigate the relationship between cultural backgrounds and patterns of Internet activity, Internet privacy concerns and online trust. In particular, this research could add cultural background, age and gender effects to the model of the calculus of the privacy concern that is proposed by Dinev and Hart (2006, pp.63-64).

3. This study acknowledges the importance of first establishing "what counts as personal information with regard to Internet users" before setting out to measure their privacy concerns and Internet trust, which is proposed by Smith *et al.* (1996, p.189). The findings from this question have explained what is 'private' in Malaysia and Saudi Arabia and shown the differences in this concept between both countries.
4. This study shows that gender, age and nationality can play important roles in the formation of the individual's online privacy perspectives, an idea proposed by Newell (1998, p. 366) and Bellman (2004, pp 313-324).
5. This study has developed and validated an instrument in English and Arabic, that is, a questionnaire for measuring the relationship between cultural factors and privacy perspectives. Both Arabic and English versions of the questionnaire could be used as a whole to compare cultural and demographic effects on the online privacy perspective using participants from different countries and religions.

9.4 RESEARCH LIMITATIONS

This research provides rich information on the multifarious relationships between the online privacy perspectives of Malaysian and Saudi Internet users and their cultural backgrounds. These diverse relationships divide into four cultural effects, which were identified as being significant. These are social norms, religious belief, Internet regulation, and IT skills and in addition, the effect of gender and age. The above four cultural effects are associated with each of the four components of online privacy perspectives: online privacy concerns, concerns about the possible misuse of the submitted personal information, online trust in information security and in the

professional handling of personal information (see sections 9.3). as with other researches, this study has limitations, particularly with regard to population samples and the questionnaire which have placed limitations upon this research. These limitations are discussed below.

Firstly, although the initial plan was to study the online privacy perspective of Muslims in three countries, Saudi Arabia, Malaysia and the UK, the researcher found difficulty in finding sufficient participants from the UK. The reason for the lack of the UK's participation was due to the required characteristics of the participants, which were be brought up in the UK, a Muslim, and a student or member of staff and from a higher education establishment. Persons who satisfy these characteristics are present in a very small percentage in the UK. There are approximately two million British Muslims in the UK of which one-third are under the age of 16 while another third have no formal qualifications (Briggs and Birdwell, 2009, p.4). The chances, therefore, finding sufficient numbers for a correctly sized representative sample in the UK was low. The researcher, therefore decided to abandon this part of the research and compare only Saudi and Malaysian populations.

Secondly, as mentioned in section (5.7.1: Target Participants), the sample population by design not only required members to be Muslim but also a student or member of staff in a higher education establishment, therefore, the results of this study are limited to the extent that university populations are representative of each country's population.

Thirdly, the questionnaire, particularly the third part, which covered the independent variables i.e. the effects of religious beliefs, social norms, Internet regulation and IT skills was designed to measure what people were actually doing with regard to their

online privacy attitudes, however, such answers, would be rather a measure of what people claim they would do.

Fourthly, using one directional hypotheses would increase the risk of having a Type III error, which is accepting of the one directional alternative whereas the other is true (Leventhal and Huynh, 1996, p.281). Further studies using the two directions and null hypothesis could confirm whether this study has the wrong direction, with or without the hypotheses.

Finally, the population of Malaysian students was limited to the Centre and West of Malaysia.

9.5 DIRECTIONS FOR FUTURE RESEARCH

This study provides an understanding of what cultural influences might most affect the privacy perspectives of Internet users in Malaysia and Saudi Arabia. Web designers working in both countries could be prompted to use such findings to consider cultural effects when designing their websites' privacy policy

This research could be a starting point for IS researchers to further study individual privacy perspectives. The following are some suggested directions for future research in the area of the cultural effects on online privacy perspectives.

1. Investigate the effect of the cultural background, age and gender on the online privacy perspective in general and on the privacy concern and Internet trust specifically in other countries including those in the Arabic World, the Far East and Western countries. This approach will provide a wider range of comparative studies into the many factors that affect individual online privacy perspectives.

2. Investigate each of the cultural influences that have been identified by this research in more detail to discover if there are any further factors or sub-factors that are involved. Such research could be done using qualitative methodology in order to study in depth each of the identified factors in depth.
3. Investigate the effect of other possible factors in order to add more variables that affect online privacy perspectives.
4. Investigate the Saudi attitude toward Internet regulation as a non-factor in forming their privacy concerns and Internet trust.
5. Investigate the gender differences between Malaysia and Saudi Arabia in their privacy concerns and Internet trust.

9.6 CONCLUSION

This thesis has investigated the online privacy perspectives of Internet users in Saudi Arabia and Malaysia and discussed whether these perspectives are culturally relevant. This research used a survey in the form of a questionnaire and compared the online privacy perspectives of Saudi and Malaysian internet users. In addition, the research examined the relationship between the effect of the cultural background of these Internet users upon their attitudes toward privacy online and their perspectives on privacy.

The research has shown that the level of concern and degree of trust found by Malaysian students with regard to submitting personal information via the Internet was affected by their social norms, which acted upon their online privacy attitudes. The level of concern and trust with regard to submitting personal information via the Internet was also related to the effect of their religious beliefs acting on their online privacy attitudes.

The other Malaysian privacy perspectives studies were mostly affected by their social norms whereas Saudi privacy perspectives were primarily influenced by their religious beliefs. The other cultural factors, i.e. the Internet regulations in force in each country and the IT skills of participants, were shown to have equal effects on both Malaysian and Saudi privacy perspectives. The findings of this research will contribute to the knowledge of web designers and Internet policy makers in Saudi Arabia and Malaysia. Because of this research they are now provided with the awareness that will enable them to consider these cultural effects when they design website privacy policies and practices.

REFERENCES:

Al-A'ali, M., (2008), "Computer ethics for the computer professionals from an Islamic point of view". In *Journal of Information, Communication & Ethics in Society*, **6**, **(1)**, pp. 28-45.

Allen R., (2000), "Body image: gender, ethnic, and age differences". *Journal Social Psychology.***140**, pp. 465–72.

Alexander, N., (2011),"Teaching Leadership to Female Students in Saudi Arabia". *Advancing women in leadership*, **31**, p. 199.

Al Lily, A. (2011), "On line and under veil: technology-facilitated communication and Saudi female experience within academia". *Technology in Society,* **33(1-2)**, pp119-127.

Alghaith, W., Sanzogni, L., and Sandhu, K., (2010), "Factors Influencing the Adoption and Usage of Online Services in Saudi Arabia". *Electronic Journal of Information Systems in Developing Countries*, **40, (1),** pp.1-32

Al-Saggaf, Y., (2004), "The Effect of Online Community on Offline Community in Saudi Arabia'. *Electronic Journal of Information Systems in Developing Countries*, **16, (2)**, pp. 1-16.

Al-Saggaf, Y., and Weckert, J., (2004), "The effects of participation in online communities on individuals in Saudi Arabia.", *ACM SIGCAS Computers and Society*, **34, (1)**

Altman, I., (1975), "*The environment and social behaviour"*. Brooks/Cole Publisher, Monterey, USA

Amin, H., and Ramayah, T. (2010), "SMS banking: Explaining the effects of attitude, social norms and perceived security and privacy". *The Electronic Journal of Information Systems in Developing Countries*, **41**.

Ajzen, I., and Fishbein, M., (1980), "Understanding attitudes and predicting social behavior". Englewood Cliffs, NJ: Prentice-Hall.

Ajzen, I., (1991), "The Theory of Planned Behaviour". *Organizational Behaviour and Human Decision Process,* **50, (2),** pp.179-211 From Baker et.al. (2007), pp. 352-375

Aycan, Z., Kanungo, R., Mendonca, M., Yu, K., and et al, (2000), "In Impact of cultural on human resource management practices: a ten-country comparison". *Applied Psychology: An International Review*, **49, (1)**, pp.192–221.

Baki, R., (2004), "Gender-segregated Education in Saudi Arabia: Its Impact on Social Norms and the Saudi Labor Market". *Education Policy Analysis Archives,* **28, (12)**, 1-12.

Baker, E., Al-Gahtani, S., and Hubona, G., (2007), "The effects of gender and age on new technology implementation in a developing country. Testing the theory of planned behavior (TPB)". In *Information Technology and People*, **20, (4**) pp.352-375

Bartel-Sheehan K., (1999), "An investigation of gender differences in on-line privacy concerns and result behaviours". *In Journal Interact Mark*, **13, (4),** p. 24

Barzilai-Nahon, K., and Barzilai, G., (2005), "Cultured technology: The Internet and religious fundamentalism." *The Information Society*, **21(1),** 25-40.

Bellman, S., Johnson, E., Kobrin, E., and Lohse, G., (2004), "International Differences in Information Privacy Concerns: A Global Survey of Consumers". *The Information Society*, **20,** pp.313-324

Bem, S. L. (1981). Gender schema theory: A cognitive account of sex typing. *Psychological review*, *88*(4), 354.

Benbasat, I., Goldstein, D., and Mead, M., (1987), "The Case Study Research Strategy in Studies of Information Systems". *MIS Quarterly*, **September,** pp. 369-386.

Berween, M., (2002), "The Fundamental Human Rights: An Islamic Perspective". *The International Journal of Human Rights*, **6**, **(1),** pp. 61-78

Bland J., and Altman, D., (1997), "Cronbach's alpha. Statistics notes." *BMJ*, pp. 314:572.

Boland, JR.(1985), Phenomenology: A Preferred Approach to Research on Information Systems. In E. MUmford, R. Hirschheim, G. Fitzgerald and T. Wood-Harper (Eds.), *Research Methods in Information System.* New York: North Holland.

Brandimarte, L, Acquisti, A., and Loewenstein, G., (2010), *Misplaced Confidences: Privacy and the Control Paradox.* Technical report, Mimeo, Carnegie: Mellon University

Bremmer, I. (2010), Democracy in Cyberspace-What Information Technology Can and Cannot Do. *Foreign Aff.*, **89**, (**86)**.

Brey, P., (2007), "Is Information Ethics Culture-Relative". *International Journal of Technology and Human Interaction*, **3, (3),** pp.12-24

Briggs, R. and Jonathan Birdwell (2009), "Radicalization among Muslims in the UK", *Microcon Working Policy Working Paper 7*

Bryman, A., (2008), *Social Research Method.* Oxford University Press, Great Clarendon Street, Oxford, OX2 6DP, England

Campanelli P., (1997), "Testing survey questions: new directions in cognitive interviewing". *Bulletin de Methodologie Sociologique*, **55**: 5–17.

Campbell, H., (2007), "Who's got the power? Religious authority and the Internet." *Journal of Computer-Mediated Communication*, **12 (3),** pp. 1043-1062.

Capurro, R., (2005), Privacy: An intercultural perspective. *Ethics and Information Technology*, **7**, pp. 37-47

Chen, L. D., Gillenson, M. L., & Sherrell, D. L. (2002), "Enticing online consumers: an extended technology acceptance perspective*". Information & Management*, **39,** pp.705–719.

Cialdini, R. B., and Goldstein, N. J., (2004), "Social influence: Compliance and conformity." *Annu. Rev. Psychol.*, **55**, pp.591-621.

Cheong, K., and Lee, K., (2009), "Counting ethnicity: The New Economic Policy and social integration". *Malaysian Journal of Economic Studies* **46(1)**, pp. 33-52

Chin, J., (2001), "Malaysian Chinese Politics in the 21st Century: Fear, Service and Marginalisation". *Asian Journal of Political Science,* 9(2): 78-94.

Clarke, R., (1999), "Internet privacy concerns; Confirm the case for intervention". *Communication of the ACM*, **42**, (2), pp.60-67

Clarke R., (2006) Introduction to Dataveillance and Information Privacy and Definitions of Terms. From http://www.cse.unsw.edu.au/~se4921/PDF/Other/roger-clarke-intro.pdf last visit 14/06/12

Cobanoglu, C., Warde, B., and Moreo, P., (2001), "A comparison of mail, fax and web based survey methods". *International Journal of Market Research,* **43, (4),** pp.441-452

Collste, G., (2008), “Global ICT-ethics: The case of privacy”. *Journal of Information, Communication and Ethics in Society,* **6, (1),** 76–87.

Conner, M., and Sparks, P., (2005), “The theory of planned behaviour and health behaviours.” *Predicting health behaviour,* **2**, pp.170-222.

Creswell, J., (2003), *Research design: Qualitative, quantitative, and mixed methods approaches*, (2nd ed.). Thousand Oaks, California: Sage Publications.

David, M., and Sutton, C., (2004), *The Basic Social Research.* SEGE Publications Ltd, 1 Oliver’s Yard, 55 City Road, London EC1Y 1SP

Davis, F.D., R.P. Bagozzi, and P.R., Warshaw, "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," *Management Science*, **35, (8),** pp.982-1003.

Darke, P., Shanks, G., and Broadbent, M., (1998), “Successfully completing case study research: combining rigour, relevance and pragmatism”. *Information Systems Journal*, **8**, pp.273–289.

DeMaio, T. J., & Rothgeb, J. M., (1996), “Cognitive interviewing techniques: In the lab and in the field”. In N., Schwarz, and S., Sudman, (Eds.), *Answering questions: Methodology for Determining Cognitive and Communicative Processes in Survey Research.* pp. 177-195). San Francisco: Jossey- Bass

Denscombe, M., (2003), *The Good Research Guide, for small-scale social research project.* Oxford University Press McGraw-Hill Education, SL6 2QL, England

De Vaus, D., (2002), *Analyzing Social Science Data.* Sage Publications, London.

Dinev, T., and, Hart, P., (2002), “Internet Privacy Concerns and Trade-Off Factors-Empirical Study and Business Implications”.Working Paper, Florida Atlantic University.

Dinev, T. and Hart, P., (2003), “Privacy concerns and Internet use – a model of trade-off factors”. *Best Paper Proceedings of Annual Academy of Management Meeting.* Seattle.

Dinev, T., and Hart, P., (2004), “Internet privacy concerns and their antecedents-measurement validity and a regression model”. *Behavior & Information Technology*, **23(6),** pp.413-422

Dinev, T., and Hart, P., (2006a), "Internet privacy and social awareness as determinants of Intention to transact". *International Journal of Electronic Commerce*, **10(2),** pp.7-29

Dinev, T., and Hart, P., (2006b), "An extended privacy calculus model for e-commerce transactions", *Information Systems Research*, **17(1),** pp.61-80

Dou, W., Lim, K., Su, C., Zhou, N., and Cui, N., (2010), "Brand positioning strategy using search engine marketing". *Management information systems quarterly* **34, (2),** pp. 261

Ehrenreich, R., (2001), "Privacy and Power". *Georgetown Law Journal*, **89 (6)**, pp. 2047-2062.

Lamer, W, (2012), "Twitter and Tyrants: New Media and its Effects on Sovereignty in the Middle East" Arab Media & Society. **16**

Larson, E., (1994), *The Naked Consumer: How Our Private Lives Become Public Commodities*. New York: Penguin.

Elgarah, W., and Falaleeva, N., (2005, August), "Adoption of biometric technology: Information privacy and TAM". In *Proceedings of the Eleventh Americas Conference on Information Systems*, pp. 1209-1212.

Elgesem, D., (1996), "Privacy, respect for persons and risk". C. ESS (Ed.) *Philosophical Perspectives on Computer-Mediated Communication*, Albany, NY: State University of New York Press, pp. 45-66

Elgesem, D., (2004)., "Structure of Right in Directive 95/46/EC on the Protection of Individuals with Regards to the Processing of Personal Data & the Free Movement of Such Data", In: Spinello, and H., Tavani, (eds) *Readings in CyberEthics*. 2nd ed, Jones & Bartlett, Sudbury, Ma, pp.418-435.

Fairweather, N. B., (2001), "Privacy in the Age of Bigger Brother". *In ETHICOMP2001,* 2, pp. 309-317.

Fern, E., (1982), "The use of focus groups for idea generation: the effects of group size, acquaintanceship and moderator on response quantity and quality". *Journal of Marketing Research*, **19,** pp. 1-13, from Morgan, 1996, pp138

Field, A., (2009), *Discovering statistics using SPSS* (3rd edition.), Sage Publications Ltd, 1 Oliver's Yard, 55 City Road, London EC1Y 1SP

Fink, A. (1995), *How to ask survey questions.* Thousand Oaks, CA: Sage Publications.

Flick, U., (2005), *An Introduction to Qualitative Research* (2nd edition). Sage Publications Ltd, 1 Oliver's Yard, 55 City Road, London EC1Y 1SP

Fried, C., (1984), "Privacy". In F. Schoeman (Ed.), *Philosophical dimensions of privacy: An anthology*. Cambridge, England: Cambridge University Press. pp.203-222

Fogel, J., and Nehmad, E., (2009), "Internet social network communities: Risk taking, trust, and privacy concerns". *Computers in Human Behavior* **25**, pp.153-160.

Gable, G., (1994), "Integrating Case Study and Survey Research Methods: An Example in Information Systems". *In European Journal of Information Systems,* **3, (2),** pp.112-126

Ganow , S, and Han, S., (2010), " Model Omnibus Privacy Statute". *University of Dayton Law Review*, *35*(3), 303.

Garbarino. E.and Strahilevitz, M., (2004), "Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation". *Journal of Business Research*, 57, pp. 768–775.

Garland, R., (1991), "The mid-point on a rating scale: Is it desirable?", *Marketing Bulletin,* **2**, pp. 66–70.

Gefen, D., Karahanna, E., and Straub, D. W., (2003), "Trust and TAM in online shopping: An integrated model." *MIS quarterly*, pp. 51-90.

Ghani, N.. A., and Sidek, Z., M., (2009), "Owner-Controlled Towards Personal Information Stored in Hippocratic Database". *Proceedings of the 2009 International Conference on Computer Technology and Development.* **November 13-15, (2),** pp 227-231, Kota Kinabalu, Malaysia,

Gliem J., and Gliem, R., (2003), "Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales". *Midwest Research to Practice Conference in Adult, Continuing, and Community Education*; **82, (8).**

Gillard, H., Howcroft, D., Mitev, N., and Richardson, H., (2008), "Missing women": Gender, ICTs, and the shaping of the global economy." *Information technology for development*, **14(4),** pp. 262-279.

Gilman, M. E. (2012). "The Class Differential in Privacy Law". *Brooklyn Law Review*, *77*(4).

Gond, J. P., Kang, N., and Moon, J., (2011), "The government of self-regulation: On the comparative dynamics of corporate social responsibility". *Economy and Society*, *40*(4), 640-671.

Grant, R., and Higgins, C., (1988), "Computerized Performance Monitors: Are They Costing You Customers?". *Journal of Sloan Management Review*, **29 (3)**, pp. 39-45

Greenhalgh T, Robert G, and Macfarlane F., (2004), "Diffusion of innovations in service organizations: systematic review and recommendations." *Milbank Q* vol. **82, (4),** pp. 581-629.

Gravetter, F.J., and Wallnau, L.B., (2009), *Statistics for the Behavioral Sciences,* Eighth Edition. Belmont: Wadsworth, Cengage Learning.

Guarda, P., and Zannone, N., (2008), "Towards the Development of Privacy-Aware Systems". *Information and Software Technology.*

Guba, E., and Lincoln, Y., (1992), *Effective evaluation: Improving the usefulness of evaluation results through responsive and naturalistic approaches.* Jossey-Bass, San Francisco, USA

Hasbullah, N., Noor, N., Isa, W., and Manaf, N., (2011), "Investigating the Privacy Policy Adoption among Malaysia E-Government Websites: Towards Conceptualizing the E-Privacy Assessment Framework". *Proceeding of the International Conference on Advanced Science, Engineering and Information Technology (ICASEIT 2011),* Bangi, Malaysia, **14-15 January 2011**

Hausmann, R., and Székely, M., (2001), "Inequality and the Family in Latin America". N. Birdsall, A C Kelley, & S Sinding (Eds), *Population Matters: Demographic Change, Economic Growth and Poverty in the Developing World.* New York: Oxford University Press.

Hausmann, R., Tyson, L., and Zahidi., S., (2010), *The Global Gender Gap Report 2010* (Switzerland: World Economic Forum).

Hayat, M.A., (2007), "Privacy and Islam: From the Quran to data protection in Pakistan". *Information and Communication Technology Law,* **16, (2),** pp.137-148

Hair, J. F., Anderson, R.E., R., Tatham L., & Black, W.C., (1998), *Multivariate Data Analysis,* 5th ed. Upper Saddle River, NJ: Prentice Hall

Hirschman, C., (1987), "The Meaning and Measurement of Ethnicity in Malaysia: An Analysis of Census Classification". *Journal of Asian Studies* **46(3)**, pp. 555-582.

Hill, C., Karen, L., Detmar, S., and El-Sheshai, K., (1998), "A Qualitative Assessment of Arab Culture and Information Technology Transfer". *Journal of Global Information Management,* **6, (3),** pp. 389-398

Hill, K., and Hughes, J., (1999), "Cyberpolitics: Citizen Activism in the age of the Internet. Rowman & Littlefield

Hofstede, G., (1984)., "The Cultural Relativity of the Quality of Life Concept". *Academy of Management Review,* **9,** pp.137-148

Howcroft, D., & Trauth, E. M., (2008), "The implications of a critical agenda in gender and IS research." *Information Systems Journal,* **18(2),** pp.185-202.

Howley, R., Rogerson, S., Fairweather, B., and Pratchett, L., (2004), "Role of information systems personnel in the provision for privacy & data protection in organisations & within information systems". *ETHICOMP2004,* **1, (1)**

Howley, R., (2007), "The role of Information Systems professionals in the provision for privacy and data protection within organisations, systems and the systems development process". *Thesis*; De Montfort University, Leicester

Hubona, G., Truex *III*, D., Wang, J., and Straub, W., (2006), "Cultural and Globalization issues impact the Organizational use of Information Technology" In Galletta, D.F., & Zhang, P. (eds.). *Human-Computer Interaction and Management Information Systems Applications.* M.E. Sharpe, Armonk, NY, From Baker et.al. (2007), pp. 352-375

Ibrahim, A., and Daing Ibrahim, D., (2006), "Significance of Cross Cultural Background on Internet Usage among University Students". *UNITAR E-JORNAL,* **2, (2),** pp.40-49

Ibrahim, R., Muslim, N., and Buang, A., (2011), "Multiculturalism and higher education in Malaysia". *Procedia: social and behavioral sciences* **15,** pp.1003.

Jankowicz, A., D., (1991), *Business Research Projects for Students*. Chapman and Hill, 2-6 Boundary Row, London SE1 8HN

Jehangir, M., Dominic, P., Naseebullah, and Khan, A., (2011), "Towards Digital Economy: The Development of ICT and E-Commerce in Malaysia". *Modern Applied Science,* **5(2).**

Johnson, T.P., (1998), "Approaches to Equivalence in Cross-Cultural and Cross-National Survey Research". *ZUMA-Nachrichten Spezial*, **January** pp.1-40

Jobe, J., and Mingay, D., (1991), "Cognition and survey measurement: History and overview". *Applied Cognitive Psychology*, **5,** pp. 175-192.

Kaplan, B., and Maxwell, J., (1994), "Qualitative Research Methods for Evaluating Computer Information Systems". *Evaluating Health Care Information Systems: Methods and Applications*, J. G. Anderson, C. E. Aydin, and S. J. Jay (eds.), Sage, Thousand Oaks, CA, pp. 45–68.

Kasim, M., Malek, M., and. Hambali, Z., (2011), "The Provision of High Speed Broadband (HSBB) in Malaysia in Enhancing Malaysian Access to Internet Applications: A Case of Telecom Malaysia". *Global Media Journal,* **5(2).**

Keesing, R. M., (1974), "Theories of culture." *Annual review of anthropology*, **3**, pp.73-97.

Kehoe, C., Pitkow, J., and Morton, K., (1997), *GVU's 8th WWW user survey.* Atlanta, GA: Graphic, Visualization, and Usability Center, Georgia Tech Research Center.

Kelly, E., and Rowland, H., (2000), "Ethics and Online Privacy Issues in Electronic Commerce". *Business Horizons,* **May-June** pp.3-12

Kemp, R and Moor, A., (2007), "Privacy". *In Library Hi Tech,* **25, (1)**, pp. 58-78

Kerlinger, F., (1986), *Foundation of Behavioral Research*, 3rd edition, Holt, Rinhart and Winston.

Khalid, H., and Mohamood, K., (1997), "Cataloguing practice in university libraries". *Asian libraries*, **6, (3/4)**, pp.155.

Kitiyadisai, K., (2005), "Privacy rights and protection: foreign values in modern Thai context". *Ethics and Information Technology*, **7**, pp. 17-26

Kluver, R., & Cheong, P. H., (2007), "Technological modernization, the Internet, and religion in Singapore.", *Journal of Computer-Mediated Communication*, **12(3),** pp. 1122-1142.

Kuthy, Daniel W., (2011), "The Effect of State Capacity on Democratic Transition and the Survival of New Democracies" *Political Science Dissertations.*

Lallmahamood, M., (2007), "An examination of individual's perceived security and privacy of the internet in Malaysia and the influence of this on their intention to

use e-commerce: Using an extension of the technology acceptance model." *Journal of Internet Banking and Commerce*, **12(3)**, pp.1-26.

Lee, A., S., (1989), "A Scientific Methodology for MIS Case Studies". *MIS Quarterly* **(13:1), March**, pp.32-50.

Lee J.S., Cho H., Gay G., Davidson B. and Ingraffea A., (2003), "Technology acceptance and social networking in distance learning". *Educational Technology and Society* **6**, pp.50–61

Lee, Y. and Kown, O., (2010), "An index-based privacy preserving service trigger in context-aware computing environments". *Expert systems with applications*, **37.7,** pp.5192.

Lessig, L., (2001). *The future of ideas: The fate of the commons in a connected world*. Random House, Inc., New York

Leventhal, L.,and Huynh, C. L., (1996), "Directional decisions for two-tailed tests: Power, error rates, and sample size". *Psychological Methods*, **1(3)** ,p. 278.

Liebermann, Y. and Stashevsky, S., (2002), "Perceived risks as barriers to Internet and e-commerce usage". *Qualitative Market Research*, **5, (2)**, pp. 291-300

Lietz, P., (2010), "Research into questionnaire design". *International Journal of Market Research* , pp. 249-272.

Lim, K., and Har, W., (2008), "Islamic state and Malaysian Chinese politics: A rhetorical study of selected Political advertisements in the local Chinese media during the 11th Malaysian general election campaign". *Journal of Politics and Law*. **1(1)**, pp. 25 – 39.

Lipton, J., (2010), "Digital Multi-Media and the Limits of Privacy Law". *Case Western Reserve Journal of International Law*, **42(3),** pp. 551-571.

Loch, K., Straub, D., and Kamel, S., (2003), "Diffusing the internet in the Arab world: The role of social norms and technological culturation". *IEEE Transactions on Engineering Management*, **50(1)**, 45-63.

Lombardi, C. M., and Hurlbert, S. H., (2009), "Misprescription and misuse of one-tailed tests". *Austral Ecology*, **34(4),** pp.447-468.

Maab, W., (2011), "The Elderly and the Internet: How Senior Citizens Deal with Online Privacy", Trepte, S. & Reinecke, L. (Eds): *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*. Springer: Heidelberg.

Malhotra, N. K., (2004), "Internet users' information privacy concerns (IUIPC): the construct, the scale and a causal model". *Information Systems Research,* **15, (4),** p. 336.

Mann, M., (1984), "The Autonomous Power of the State", *Archives Européennes de Sociologie*

25(2): 185–212.

Margulis, T., (2003), "Privacy as a social issue and behavioural concept". *Journal of Social Issues,* **59, (2),** pp. 243.

Margulis, T., (2011), "Three Theories of Privacy: An Overview". In Trepte, S., & Reinecke, L. (Eds.), *Privacy online: perspectives on privacy and self-disclosure in the social web*. Springer-Verlag, New York

Marshall, N., (1974), "Dimensions of Privacy Preferences", *Multivariate Behavioral Research,* **9 (July)**, 252-271.

McRobb, S., (2006). "Let's Agree To Differ: varying interpretations of online privacy policies". *Journal of Information, Communication & Ethics in Society,* **4**, **(4),** pp. 2/5-228.

Milberg, S. J., Burke, S. J., and Smith, H. J., (1995), "Values, Personal Information Privacy, and Regulatory Approaches". *Communications of the ACM*, **(38:12),** pp. 65-74.

Milberg, S. J., Smith, H. J., and Burke, S. J., (2000), "Information Privacy: Corporate Management and National Regulation," *Organization Science*, (11:1), pp. 35-57.

Miller, A., (1971), *The assault on privacy: Computers, data banks and dossiers*. University of Michigan Press, Ann Arbor, USA

Mitchell, I. D., (2012),Third-Party Tracking Cookies and Data Privacy Available at SSRN:http://ssrn.com/abstract=2058326or http://dx.doi.org/10.2139/ssrn.2058326

Moor, J., (1985), "What is Computer Ethics?" *Metaphilosophy,* **16, (4),** pp. 266-275.

Moor, J., (2001), "The future of computer ethics". *Ethics and Information Technology,* **3**. pp.89-91

Moor, J., (2002), "Toward a theory of privacy in the information age". In Bynum and Rogerson. *Computer Ethics & Professional Responsibility,* pp.249-262, Blackwell, Oxford

Moore, N., (2002), *How to do research, The Complete Guide to Designing and Managing Research Projects*. Facet Publishing, 7 Ridgmount Street, London WCIE 7AE, England

Moores, T., (2005), "Do Consumers Understand the Role of Privacy Seals in E-Commerce?". *Communications of The ACM*, **48, (3),** pp.86-91

Morgan, D.L., (1996), "Focus groups". *Annual review of sociology*

Morgan, D.L., (1998), "*Planning Focus Groups".* Thousand Oake, Clif: SAGE, from Bryman, 2001, p. 341

Nakada, M., and Tamura, T., (2005), "Japanese conceptions of privacy: An intercultural perspective". *Ethics and Information Technology*, **7**, pp. 27-36

Newell, P.B., (1998), "A Cross-Cultural Comparison of Privacy Definitions and Functions: A System Approach". *Journal of Environmental Psychology*, **18,** pp. 357-371

Norman, G., (2010), "Likert scales, levels of measurement and the "laws" of statistics." *Advances in health sciences education*, **15(5),** pp.625-632.

Nunnally, J., (1967), *Psychometric theory.* New York: McGraw-Hill

Oates, B., (2005), *Researching information systems and computing*. SAGE, London.

Oliver, P., (2003), *The Student's Guide to Research Ethics*. Open University Press McGraw-Hill Education, SL6 2QL, England

Ooi, T., Ho, H., and Amri, S., (2010), "Education websites and their benefits to potential international students: a case study of higher education service providers in Malaysia". *Current Issues in Education,* **13(1).**

Orlikowski, W., and Baroudi, J., (1991), "Studying information technology in organizations: research approaches and assumptions", *Information Systems Research*, **2 (1),** pp. 1-28.

Orito, Y., Murata, K., McRobb, S., and Adams, A., (2008), "Privacy online and Culture: Evidence from Japan". *ETHICOMP2000.*

Pallent, J., (2001), *SPSS Survival Manual.* SPSS Inc., Chicago, USA.

Payne, S., Field, D., Rolls, L., Hawker, S., and Kerr, C., (2007), "Case study research methods in end of life care practice: reflections on three studies". *Journal of Advanced Nursing*, **58 (3)**, pp. 236-245

Pawson, R., (2000), “Methodology”. In Tayler, S. (Ed.), *Sociology Issues and Debates.* Palgrave, Houndmills, Basingstoke, Hampshire, RG21 6XS and 175 Fifth Avenue, New York, N.Y. 10010

Peterson K., and Siek K.,(2009), “Analysis of information disclosure on a social networking site2, in AA Ozok & P Zaphiris (eds), *Online Communities*, pp. 256-264. Springer-Verlag, Berlin

Peterson, E., and Ulferts, G., (2011), "Government Control Of Communications Technology". *The international business and economics research journal*, **8, (9)**

Ponterotto, J., (2005), “Qualitative research in counselling psychology: A primer on research paradigms and philosophy of science”. *In Journal of Counselling Psychology* **52 (2),** pp.126-136.

Premkumar, G., and Ramamurthy, K., (1995), “The role of interorganizational and organizational factors on the decision mode for adoption of interorganizational systems”. *Decision Sciences,* **26(3),** 303–336.

Presser, S., Couper, M., Judith, L., Martin, E., and *et al*, (2004), “Methods for Testing and Evaluating Survey Questions”. *Public Opinion Quarterly*. **68(1),** pp. 109–30.

Roni, N., Napiah, M., and, Hassan, B., (2011), *Impact of ICT on Privacy and Personal Data Protection in Two Malaysian Academic Libraries*: Asia-Pacific Conference On Library & Information Education & Practice: Issues, Challenges and Opportunities

Ruane, J., (2005), *Essentials of research methods: A guide to social science research.* Blackwell, Malden, MA

Saint-Germain, M., Bassford, T., and Montano, G., (1993), “Survey and focus group in health research with older Hispanic women”. *Qualitative eHealth Research,* **3,** pp. 341-367, from Morgan, D.L., (1996), pp137

Sarantakos, S., (2005), *Social research*, 3rd ed, Palgrave Macmillan, Basingstoke, UK.

Saudi, M., Ismail, S., Tamil, M., and Idris, M., "Phishing: Challenges and Issues in Malaysia". *The International Journal of Learning*, **14**, pp. 79-88, 2007

Schwartz, S. H., (2006), “A theory of cultural value orientations: Explication and applications.” *Comparative sociology*, **5(2-3),** pp.2-3.

Seawright, J. and Gerring. J., (2008), "Case Selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Options". *Political Research Quarterly*, **61 (2)**, pp. 294 -308.

Seničar, V. Blazič, B., and Klobučar, T., (2003), "Privacy-Enhancing Technologies-approaches and development". *Computer Standards and Interfaces*, **25,** pp.147-158

Shalhoub, Z., (2006a), "Trust, privacy & security in electronic business: the case of the GCC Countries". *Information Management and Computer Security*, **14, (3),** pp.270-283

Shalhoub, Z. (2006b), "Content Analysis of Web Privacy Policies in the GCC Countries". *Information Systems Security*, **July/August**, pp.36-45

Siala, H., O'Keefe, R., and Hone, K., (2004), "The impact of religious affiliation on trust in the context of electronic commerce." *Interacting with Computers*, **16**, 7–27

Silverman, D., (2005), *Doing Qualitative Research*. SEGE Publications Ltd, 1 Oliver's Yard, 55 City Road, London EC1Y 1SP

Slovic, P., Malmfors, T., Mertz, C.,Neil, N., and Purchase, F., (1997), "Evaluating chemical risks: results of a survey of the British toxicology society". *Human and Experimental Toxicol*, **16**, pp.289–304.

Skinner, G., Han, S., and Chang, E., (2005), "A new conceptual framework within information privacy: Meta privacy". *Centre for Extended Enterprises and Business Intelligence*.

Skinner, G., Han, S., and Chang, E., (2006), "An information privacy taxonomy for collaborative environments". *Information Management & Computer Security*, **14, (4),** pp.382 – 394

Smith, H., Milberg, S., and Burke, S., (1996), "Information Privacy: Measuring Individuals' Concerns about Organizational Practices". *MIS Quarterly: Management Information System*, **20**, pp.167.

Smith, P. B., Torres, C. V., Hecker, J., Chua, C. H., Chudzikova, A., Degirmencioglu, S., and Yanchuk, V., (2011), "Individualism–collectivism and business context as predictors of behaviors in cross-national work settings: Incidence and outcomes." *International Journal of Intercultural Relations*, **35(4),** pp.440-451.

Solove, D., (2013), "Privacy Self-Management and the Consent Paradox". *Harvard Law Review, 126.*

Spiekermann, S., and Cranor .F., (2009), "Engineering privacy". *IEEE Transactions on Software Engineering.* 35, pp. 67-82.

Stahl, B., (2004), "Responsibility for Information Assurance and Privacy". *Journal of Organizational and End User Computing*, **16**, (3), pp. 59 - 77

Stahl, B., (2008), "The Impact of the UK Human Rights Act 1998 on Privacy Protection in the Workplace". In Subramanian, R (Ed.), *Computer Security, Privacy, and Politics: Current Issues, Challenges, and Solution*, Idea Group, Hershey, PA, pp.55-68

Stahl, B., and Elbeltagi, I., (2004), "Cultural Universality versus Particularity in CMC". *Journal of Global Information Technology Management*, **7**, pp. 47-65.

Steele, J., Bourke, L., Luloff, A., Liao, P., Theodori, G., and Krannich, R., (2001), "The drop-off/ pick-up method for household survey research". *Journal of the Community Development Society*, **32**, pp. 238-250.

Steward, K., Segars, A., (2002), "An empirical examination of the concern for information privacy instrument". *Inform. Systems Res.* **13(1).** pp. 36–49.

Stone, E., Gueutal, H., Gardner, D., and McClure, S., (1983), "A field experiment comparing information-privacy values, beliefs and attitudes across several types of organizations". *Journal of Applied Psychology*, **68**, pp. 459- 468.

Straub, D., Boudreau, M., and Gefen, D., (2004), "Validation Guidelines for IS Positivist Research". *Communications of the AIS* **(13),** pp. 380-427

Tabachnick, B., and Fidell, L., (2007), *Using multivariate statistics* (5th ed.). Needham Heights, MA: Springer.

Tavani, H., and Moor, J., (2004), "Privacy Protection, Control of information, and Privacy-Enhancing Technology". In: Spinello & H. T. Tavani (Eds.), *Readings in CyberEthics* 2nd edition, Jones & Bartlett, Sudbury, Ma. pp.436-449

Tavani, H., (2007), "Philosophical theories of privacy: Implications for an adequate online privacy policy". *Metaphilosophy.* **38**, 1-22.

Tavani, H., (2008), "Informational privacy: concepts, theories and controversies". In K.E. Himma & H.T. Tavani (EDS), *The Handbook of Information and Computer Ethics*. Hoboken, N.J., Wiley

Tourangeau, R., (1984), “Cognitive Science and Survey Methods”. In T.B. Jabine, M.L. Straf, J.M. Tanur, and R. Tourangeau (Eds), *Cognitive Aspects of Survey Methodology: Building a Bridge between Disciplines*, Washington, DC: National Academy Press, pp. 73-100.

Tourangeau, R., and Rasinski, K., (1988), "Cognitive processes underlying context effects in attitude measurement". *Psychological Bulletin* **103**, pp. 299-314.

Vasalou, A., Gill, A., Mazanderani, F., and Joinson, A., (2011), “Privacy dictionary: A new resource for the automated content analysis of privacy”. *Journal of the American Society for Information Science and Technology*. **62**, pp. 2095-2105.

Volkman, R., (2003)., “Privacy as life, liberty, property”. *Ethics and Information Technology*. **5**, pp.199-210.

Walsham, G., (1993), *Interpreting Information Systems in Organizations*. Wiley, Chichester.

Walsham, G., (2006), “Doing interpretive research”. *European Journal of Information Systems*, **15.3**

Walther, Joseph B., (2011), “Introduction to Privacy Online”, Trepte, S. & Reinecke, L. (Eds): *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*. Springer: Heidelberg.

Ward, V., Bertrand, J., and Brown, L., (1991), “The comparability of focus group and survey result”. *Evaluation Review,* **15,** pp. 266-28, from Morgan, D.L pp136

Warren, S., L., Brandeis, (1890), “The right to privacy”. *Harvard Law Review*. **4(1),** pp. 193–220.

Weckert, J., and Adeney, D., (1997), *Computer and Information Ethics.* Greenwook Press, Westport.

Westin, A., (1967), *Privacy and Freedom.* Atheneum, New York

Westin, A., (2001), “Opinion Surveys: What Consumers Have To Say About Information Privacy: Testimony before U.S. House of Representatives, Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection’’ May 8.

Wight, D., (1994), “Boys’ thoughts and talk in a working class locality of Glasgow”. *Sociological Review,* **42**, pp. 703-737.

Wilford, S., (2004), "Information & communication technologies, privacy & policies: an analysis from the perspective of the individual". *Thesis*; De Montfort University

Willis, G. DeMaio, T., and Harris-Kojetin, B., (1999), "Is the Bandwagon Headed to the Methodological Promised Land? Evaluation of the Validity of Cognitive Interviewing Techniques". In M. Sirken, D. Herrmann, S. Schechter, N. Schwarz, J. Tanur and R. Tourangeau (Eds.), *Cognition and Survey Research*. Wiley, New York

Wirtz, J., Lwin, M., and Williams, J., (2007), "Causes and consequences of consumer online privacy concern". *International Journal of Service Industry Management,* **18, (4),** pp. 326-348

Wright, K., (2004), "On-line relational maintenance strategies and perceptions of partners within exclusively Internet-based and primarily Internet-based relationships". *Communication Studies,* **55 (2),** pp. 418–432

Xu, H., Dinev, T., Smith, H. J., and Hart, P., (2008), "Examining the formation of individual's

information privacy concerns: toward an integrative view". *In Proceedings of 29th Annual International Conference on Information Systems (ICIS 2008)*, Paris, France

Xue, S., (2005)., "Internet policy and diffusion in China, Malaysia and Singapore". *Journal of Information Science*, **31(3),** 238–250.

Yao-Huai, L., (2005). "Privacy and Data Privacy Issues in Contemporary China". *Ethics and Information Technology*. **7**, pp. 7-15.

Yao, M., (2011), "Self-Protection of Online Privacy: A Behavioral Approach", Trepte, S. & Reinecke, L. (Eds): *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*. Springer: Heidelberg.

Yang, C. K., (1966). *Chinese community society: The family and the village.* MIT Press, Cambridge.

Zaaba, Z., Aning, A., Gunggut, H., Ramadan, F., and Umemoto, K., (2010), "English as a Medium of Instruction in the Public Higher Education Institution: A Case Study of Language-in-Education Policy in Malaysia," in *Selected Topics in Education and Education Technology*,H. Fujita, and J. Sasaki, Eds. Iwate: WSEAS press, pp. 188-196.

Zakaria, N., Stanton, J., and Sarkar-Barney, S., (2003), "Designing and implementing culturally sensitive IT applications. The interaction of culture values and privacy issues in the Middle East". *Information Technology and People,* **16, (1),** pp. 49-75

Zeller, R., and Carmines, E., (1980), *Measurement in the Social Sciences*, Cambridge University Press, London.

Ziegler, M., (2011), "Applicant faking: A look into the black box". *The Industrial organizational psychologist* **49, 1**.

Zukowski, T., Brown, I., (2007), "Examining the influence of demographic factors on Internet users' information privacy concerns", *SAICSIT '07: Proceedings of the 2007 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries*, ACM, New York, NY, USA, pp. 197–204.

Electronic References:

http://ksa.daralhayat.com/ksaarticle/337566, on 10/12/2011 last visit 07/03/2012

http://www.emirates247.com/news/region/saudi-ministries-asked-not-to-take-women-s-mobile-number-2011-12-11-1.432186 on 10/12/2011 last visit 14/06/2012

APPENDIX A: Focus Group Invitation Letter

Dear …….

This letter is to give you information in the hope that you will contribute to my research at De Montfort University, in Leicester, England.

This research would contribute to knowledge by providing an analysis of the influence of cultural background of individuals on their perspective toward privacy within internet activities.

As a result of your contribution I will:

1. Gain knowledge of the cultural influences that affect the perspective of individuals toward privacy within internet usage.
2. Find out similarities and differences of individual perspectives of Muslims with different cultural backgrounds, towards privacy and internet usage.
3. Improve the next focus groups
4. be able to prepare my questionnaire survey as the main research methodology in my research

Participation in this study is entirely voluntary. It will involve an hour focus group interview for a group of 4-6 participants (Mix of Arabic and Western, as will as Male and Female), follow by a 2 side A4 feedback questionnaire on the quality of this focus group, its structure, its moderator, and so on. You may decide not to answer any of the questions if you wish. You may also decide to withdraw from this study at any time (by

advising Mr. Jehad Al-Amri[1]) and also I assure you that I will not seek any further contact with you about this unless you ask me to.

Notes collected during this study will be retained for 10 years after complete this research period [2] (i.e. 2020/2021) in a secure location and then destroyed. The information gained from this research will only be used for the above objectives, will not be used for any other purpose and will not be recorded in excess of what is required.

I may present the study findings to the Conferences, Journals, and Information Society Doctoral Programme Committees, only my supervisors, Dr. Ben Fairweather and Dr. Richard Howley, my thesis examiners and I will have access to the questionnaire data itself. There are no known or anticipated risks to you as a participant in this study.

The focus groups will take place in one of the Syndicate rooms at the Kimberlin library - De Montfort University on **one** of the following date and time:

1. Friday 16 January between 6.30 - 7.30 pm
2. Saturday 17 January between 2.30 - 3.30 pm
3. Monday 19 January between 6.30 - 7.30 pm
4. Tuesday 20 January between 6.30 - 7.30 pm
5. Thursday 22 January between 6.30 - 7.30 pm

If you are interested in participating in the next focus group please replay to me by the coming Monday 13 January 2009, with two of the most convenient date and time for you from the list above, and I will back to you by Wednesday 14 January.

For example if you are interested in participating and you can do the focus groups on Monday 19 January between 6.30 - 7.30 pm as a first convenient option, or Friday 16 January between 6.30 - 7.30 pm as a second option, please e-mail me back with this message (yes, 3, 1)

If you have any questions regarding this study or would like additional information please ask me before, or after completing the focus groups. I can assure you that this study has been reviewed and approved by my supervisors. Thank you for your assistance in this project.

Yours sincerely,

Jehad Al-Amri

---

[1] At this e-mail address: ism04ja@hotmail.co.uk

[2] According to Montfort University's regulation

APPENDIX B: **THE QUESTIONNAIRE**

APPENDIX C: **COGNITIVE INTERVIEWS**

Q	Participant 1	Participant 2	Participant 3	Participant 4
1				
2				
3	I do not understand this question. (There should be a clear sign that, now, we start new set of questions, i.e. new section with new numbering)	The location of the internet usages scale was confusing as she thought that I am asking about the level of internet usages in general (but I explain that this scale for the following questions, so modification on the structure are needed, i.e. start these questions in a new section)		
4	The description of the category at this question was not mach with the examples (i.e. "Using email required submitting personal information")		Unlike participent1, she looked at the examples and not confused by the description of the category at this question.	
5		Some explanation was needed to clarify the different between this internet activity and the previous one.		
6			She was not sure about this one, and at the beginning, she assumed it is like Amazon.com	
7				
8				
9	YouTube and Wikipedia	YouTube, watching TV and read news.	YouTube (How she see it, these	

			questions about financial websites, but there are other activities, like entertainment, games, YouTube)	
10	What kind of misused? What comes to your mind? Somebody attack my account.	Misused by others, right?		
11	..for example of MSN.	This related to previous one? (Check this)	She gave examples of the Facebook and how putting silly things in the Facebook, and how employers can use it to know about the new employees. (Check this)	
12	.. for example my bank account, and picture of me and my family.			
13			She thinks that this question is similar to question 12	
14			".. depends on the website"	
15	Not clear, if it is official (by law), like security/IT departments, it is OK! But if others, No.		She thinks that only people who did something wrong would be concerned	
16				
17	Not clear		"..depends on who are you, if you are FPI or something like that"	
18				
19	Again, who are others, no problem with authority (OK!)			

	but without authority, no!			
20	Unexpected problems, like what? (for example, when you go to a website, something come to your mind that some harm, could happened to me)		"What do you mean by unexpected problems?" (Hacking on your account, and know about you and use it against you)	
21	Do you mean that my name/credit card/address, yes, so with authority/visa/eBay? Do you feel that you gave up privacy? No not with them, because they are secure.		"What do you mean by that? Is it like credit card detailes, if it is trusted website I am not concern"	
22	He assume I am talking about MSN messenger and Skype.			
23	He differentiates between business, company and bank, but in general he could not decide to agree or not.			
24		First what is Personal Information? Need to be clear. Also there are different between general website and authorized one. (So I think that I need to add set of questions to identify what is the personal information when using internet from the perspective of each participant).	"... but what is reliable?"	
25			".. depend on what website"	
26				
	What do you mean by			

27	unknown individuals? Are they people or agents like commerce			
28				
29	Again it is different between different websites.			
30		Not all of them		
31		She seems not sure (i.e. what is the internet website). (Check this)		
32	A repeated question.			
33	Not clear to him. What they trust to submit it to the internet (Check this)			
34		I do not trust them		
35	He thinks that I am asking whether the privacy of "my friends and family" is a part of my privacy. So I need to express to the participants that I am interested in whether "my family and friend" affect the idea of privacy, not whether they are part of my privacy			
36				
37				
38				
39	Agree to strongly agree			
40				
41				

42				
43	He did not know, if there is a law for privacy.	(Thinking for moments, then asked if there is any regulation)		
45				
46	There is no internet regulation, leges...	No information.		
47				
48				
49		I do have to be more careful because I do not have the technical skills that help me to protect my privacy.		
50	Was not clear. (So I need to state first the four suggested affects; cultural, religion, regulation, and IT, and then ask if there are more affects in their mind)	Was not clear so I gave her examples of the four factors, and ask if there is any more? She added that her feeling also would play role, i.e. not feeling comfortable means not do it.		
51				
52				
53				

APPENDIX D: **CONSENT LETTER AND THE DATA COLLECTION PROTOCOL**

APPENDIX D1: CONSENT LETTER

Privacy Perspectives within Internet Usage: Study of Cultural Influences

Dear Participant

This letter is to give you information in the hope that you will contribute to my research at De Montfort University, in Leicester, England

This research would contribute to knowledge by providing an analysis of the influence of cultural background of individuals on their perspective toward privacy within internet activities.

As a result of your contribution I will:

1- **Gain knowledge of the cultural influences that affect the perspective of individuals toward privacy within internet usage.**
2- **Find out similarities and differences of individual perspectives of Muslims with different cultural backgrounds, towards privacy and internet usage.**

Participation in this study is entirely voluntary. It will involve completing a questionnaire of 8 pages. You may decide not to answer any of the questions if you wish. You may also decide to withdraw from this study at any time by advising Mr. Jehad Al-Amri[4]. I will not seek any further contact with you about this unless you ask me to.

Notes collected during this study will be retained for 10 years after complete this research period (i.e. 2020/2021) in a secure location and then destroyed[5] . The information gained from this research will only be used for the above objectives, will not be used for any other purpose and will not be recorded in excess of what is required.

I may present the study findings to the Conferences, Journals, and Information Society Doctoral Programme Committees, only my supervisors, Dr. Ben Fairweather and Dr. Richard Howley, my thesis examiners and I will have access to the questionnaire data itself. There are no known or anticipated risks to you as a participant in this study.

If you have any questions regarding this study or would like additional information please ask me before, or after completing the questionnaire. I can assure you that this study has been reviewed and approved by my supervisors. Thank you for your assistance in this project.

Yours sincerely,
Jehad Al-Amri

---

[4] At this e-mail address: jalamri@dmu.ac.uk
[5] According to De Montfort University's regulation

APPENDIX D1: THE DATA COLLECTION PROTOCOL IN ENGLISH AND ARABIC

Dear research co-operator

Thank you for your assistance on my PhD research at De Montfort University, in Leicester, England,

Please would you assist me in this by distributing to and collecting the questionnaires from the target participants?

In order to maintain the validity and reliability of my research, Please follow the research protocols indicated below:

First: Objectives of the study

This research will contribute to knowledge by providing an analysis of the influence of the cultural backgrounds of individuals on their perceptions of privacy within internet activities.

As a result of the participants contribution the research will:

Gain knowledge of the cultural influences that affect the perspective of individuals toward privacy within internet usage.

Find out similarities and differences of individual perspectives of Internet users with different cultural backgrounds, towards privacy and internet usage.

Second: Target Participants

Target participants must be a Saudi students or members of staff at one of the Saudi Arabian Universities at the time of conducting this research[6].

Third: Participation

Participation on this research will involve completing a questionnaire of 8 pages.

Fourth: Participation Procedure

The research co-operator could distribute the questionnaires before or at the end of some lectures/ meetings at their university/ college, and then collect them later at the same lecture/ meeting or at the next available ones.

Fifth: Participants' Rights

The research co-operator will also need to clarify the following information regarding the participants' rights:

Participation in this study is entirely voluntary.

Participant may decide not to answer any of the questions if they wish.

Participant may decide to withdraw from this study at any time by advising the researcher[7].

There must be no adverse consequences for participants for failing to participate or for withdrawing.

The researcher will not seek any further contact with the participants about this questionnaire or the research unless they request such contact.

Notes collected during this study will be retained in a secure location for 10 years after the completed research period (i.e. 2020/2021) and then destroyed[8] .

---

[6] Sstarting on the 25th of September 2010 and last for 4 weeks

[7] Mr. Jehad Al-Amri at this e-mail address: jalamri@dmu.ac.uk

[8] According to De Montfort University's regulation

The information gained from this research will only be used for the above objectives, will not be used for any other purpose and will not be recorded in excess of what is required.
The researcher may present the study findings to Conferences, Journals, and Information Society Doctoral Programme Committees,
Only the researcher, his supervisors[9], and his thesis examiners will have access to the questionnaire data itself.
There are no known or anticipated risks to you as a participant in this study.
Finally
If you have any questions regarding this study or would like additional information please ask me before starting to distribute the questionnaire.
Yours sincerely,
Jehad Al-Amri Centre for Computing and Social Responsibility Faculty of Technology De Montfort Universit

أخي الفاضل / أختي الفاضلة
السلام عليكم ورحمة الله وبركاته
في البدء أود أن اشكركم على الموافقة على المساعدة في بحثي المعد للحصول على درجة الدكتوراة بجامعة ديمونت فورت، بمدينة ليستر بإنجلترا.
مساعدتكم ستكون بتوزيع الإستبانات المرسلة إليكم على المشاركين المستهدفين بهذه الدراسة، ثم إعادة تجميعها بعد تعبئتها من قبل المشاركين، ومن ثم إعادتها إلي.
ولتحقيق الشرعية والمصداقية لهذا البحث، أرجوا من حضراتكم مراعات التالي قبل وأثناء توزيع الإستبانات:
أولاً أهداف الدراسة:
يهدف هذا البحث إلى الإضافة للمعرفة الأكاديمية بتحليل تأثير الخلفية الثقافية للأفراد على وجهة نظرهم تجاه مستوى الخصوصية خلال استخدام الإنترنت وبالتالي:
1 - معرفة العوامل الثقافية التي تؤثر على وجهة نظر الأفراد نحو قضايا الخصوصية خلال استخدامهم للإنترنت.
2 - معرفة أوجه التشابه والاختلاف في وجهات نظر الفرد المسلم من مختلف الثقافات نحو قضايا الخصوصية خلال استخدامهم للإنترنت

ثانياُ الفئات المشاركة في هذه الدراسة:
الفئات المستهدفه بهذه الدراسة هم الطلاب والطالبات و أعضاء هيئة التدريس والموظفيين السعوديين بالجامعات السعودية

ثالثاُ طريقة المشاركة بهذه الدراسة:
المشاركة في هذه الدراسة تشتمل فقط الإجابة على الاستبانة المكونة من 9 صفحات.

رابعاً طريقة توزيع الإستبانات:
يتم توزيع الإستبانات على المشاركين مع بداية أو قبل إنتهاء أحد او عدد من المحاضرات او الإجتماعات داخل الحرم الجامعي ثم إعادة تجميعها بعد تعبئتها من قبل المشاركين في نفس وقت اللقاء أو في أقرب لقاء ممكنة.

خامساً حقوق المشاركين بهذه الدراسة:
يتم التوضيح المعلومات التالية لجميع المشاركين بهذه الدراسة وذلك بخصوص حقوقهم كمشاركين بالدراسة:
المشاركة هي عمل تطوعي تماما.
من حق المشارك عدم الرد على أي من الأسئلة إذا رغب في ذلك.
يمكن للمشارك أيضا الانسحاب من هذه الدراسة في أي وقت
لن يتم الاتصال بالمشاركيين مرة أخرى للحصول على معلومات إضافية

[9] **Dr. Ben Fairweather, Dr. Richard Howley and Dr. Sara Wilfrod,**

APPENDIX E: **STATISTICS TABLES FOR CHAPTER 6: DESCRIPTIVE ANALYSIS**

Factor analysis validity and reliability tests

Table 6.12: Factor analysis validity and reliability tests Saudi Arabia

Variables		Inter-item correlation matrix –Saudi Arabia											KMO	Reliability
		1	2	3	4	5	6	7	8	9	10	11		
DPI	DPI1	1.00											0.843	0.659
	DPI1	0.34	1.00											
	DPI1	0.36	0.16	1.00										
	DPI1	0.04	0.58	-0.01	1.00									
	DPI1	0.07	0.55	0.09	0.74	1.00								
	DPI1	0.39	0.02	0.39	-0.13	-0.07	1.00							
	DPI1	0.07	0.50	0.06	0.62	0.61	-0.02	1.00						
	DPI1	-0.1	0.47	-0.14	0.69	0.63	-0.23	0.62	1.00					
	DPI1	0.31	-0.16	0.35	-0.34	-0.29	0.57	-0.29	-0.49	1.00				
	DPI1	0.22	-0.23	0.29	-0.41	-0.36	0.50	-0.37	-0.53	0.80	1.00			
	DPI1	0.16	0.12	0.18	0.09	0.10	0.19	0.05	0.09	0.25	0.26	1.00		
PC-1		1	2	3	4	5	6	7	8	9	10	11	0.822	0.780
	PC-11	1.00												
	PC-12	0.44	1.00											
	PC-13	0.31	0.44	1.00										
	PC-14	0.29	0.45	0.60	1.00									
	PC-15	0.36	0.28	0.32	0.34	1.00								
	PC-16	0.22	0.38	0.44	0.44	0.29	1.00							
	PC-17	0.13	0.38	0.41	0.41	0.32	0.57	1.00						
	PC-18	0.19	0.38	0.43	0.44	0.30	0.57	0.65	1.00					
	PC-19	0.23	0.14	0.11	0.23	0.14	0.13	0.01	0.10	1.00				
	PC-110	0.23	0.06	-0.01	0.12	0.11	-0.0	-0.1	-0.0	0.61	1.00			
	PC-111	0.21	0.00	-0.06	0.05	0.10	-0.2	-0.2	-0.1	0.47	0.64	1.00		

PC-2		12	13	14	15	16	17	18	19					0.931	0.958
	PC-112	1.00													
	PC-113	0.68	1.00												
	PC-114	0.60	0.80	1.00											
	PC-115	0.57	0.76	0.81	1.00										
	PC-116	0.58	0.74	0.77	0.87	1.00									
	PC-117	0.59	0.72	0.83	0.79	0.79	1.00								
	PC-118	0.60	0.77	0.81	0.78	0.78	0.83	1.00							
	PC-119	0.56	0.73	0.80	0.75	0.72	0.83	0.85	1.00						
IT1		1	2	3	4	5	6	7	8	9	10	11		0.813	0.776
	DIT1	1.00													
	DIT2	0.49	1.00												
	DIT3	0.29	0.46	1.00											
	DIT4	0.39	0.50	0.57	1.00										
	DIT5	0.37	0.40	0.40	0.39	1.00									
	DIT6	0.23	0.37	0.37	0.36	0.41	1.00								
	DIT7	0.22	0.40	0.34	0.31	0.36	0.52	1.00							
	DIT8	0.05	0.14	0.19	0.20	0.15	0.26	0.32	1.00						
	DIT9	0.26	0.22	0.23	0.32	0.22	0.21	0.20	0.16	1.00					
	DIT10	0.26	0.16	0.07	0.20	0.16	0.09	0.03	0.02	0.59	1.00				
	DIT11	0.27	0.14	0.10	0.22	0.16	0.05	0.00	0.01	0.47	0.74	1.00			
IT2		12	13	14	15	16	17							0.762	0.775
	DIT12	1.00													
	DIT13	0.39	1.00												
	DIT14	0.31	0.59	1.00											
	DIT15	0.44	0.38	0.34	1.00										
	DIT16	0.16	0.36	0.43	0.36	1.00									
	DIT17	0.13	0.31	0.41	0.37	0.58	1.00								

SN		1	2	3	4		0.787	0.823
	INDSN1	1.00						
	INDSN2	0.66	1.00					
	INDSN3	0.44	0.54	1.00				
	INDSN4	0.54	0.56	0.48	1.00			
RB		1	2	3	4		0.764	0.837
	INDRB1	1.00						
	INDRB2	0.75	1.00					
	INDRB3	0.43	0.51	1.00				
	INDRB4	0.56	0.60	0.52	1.00			
IR		1	2	3	4		0.801	0.847
	INDIR1	1.00						
	INDIR2	0.66	1.00					
	INDIR3	0.54	0.60	1.00				
	INDIR4	0.50	0.62	0.57	1.00			
ITS		1	2	3	4		0.793	0.856
	INDITS1	1.00						
	INDITS2	0.71	1.00					
	INDITS3	0.52	0.62	1.00				
	INDITS4	0.54	0.59	0.60	1.00			

Table 6.13: Factor analysis validity and reliability tests Malaysia

Variables		Inter-item correlation matrix –Malaysia											KMO	Reliability
		1	2	3	4	5	6	7	8	9	10	11		
DPI	DPI1	1.00											0.797	0.724
	DPI1	0.36	1.00											
	DPI1	0.39	0.23	1.00										
	DPI1	0.03	0.50	-0.07	1.00									
	DPI1	0.00	0.47	-0.07	0.80	1.00								
	DPI1	0.30	0.19	0.33	0.00	0.05	1.00							
	DPI1	0.18	0.27	0.19	0.32	0.33	0.20	1.00						
	DPI1	-0.05	0.42	-0.14	0.76	0.80	-0.09	0.30	1.00					
	DPI1	0.35	0.04	0.34	-0.20	-0.20	0.29	0.10	-0.31	1.00				
	DPI1	0.38	0.02	0.40	-0.25	-0.26	0.40	0.14	-0.35	0.77	1.00			
	DPI1	0.14	0.21	0.02	0.28	0.33	0.18	0.11	0.32	0.18	0.16	1.00		
PC-11		1	2	3	4	5	6	7	8	9	10	11	0.843	0856
	PC-11	1.00												
	PC-12	0.11	1.00											
	PC-13	0.22	0.47	1.00										
	PC-14	0.09	0.53	0.46	1.00									
	PC-15	0.26	0.21	0.28	0.25	1.00								
	PC-16	0.02	0.52	0.38	0.50	0.24	1.00							
	PC-17	-0.02	0.50	0.39	0.50	0.27	0.70	1.00						
	PC-18	0.06	0.45	0.33	0.53	0.28	0.57	0.68	1.00					
	PC-19	0.09	0.32	0.25	0.35	0.24	0.45	0.50	0.53	1.00				
	PC-110	0.11	0.29	0.23	0.27	0.20	0.33	0.40	0.37	0.71	1.00			
	PC-111	0.14	0.18	0.19	0.25	0.26	0.21	0.26	0.33	0.50	0.67	1.00		
DICP2		12	13	14	15	16	17	18	19				0.921	0.930
	PC-112	1.00												
	PC-113	0.52	1.00											
	PC-114	0.45	0.69	1.00										
	PC-115	0.37	0.58	0.80	1.00									
	PC-116	0.35	0.49	0.69	0.71	1.00								
	PC-117	0.43	0.58	0.70	0.73	0.80	1.00							
	PC-118	0.43	0.61	0.75	0.76	0.76	0.77	1.00						
	PC-119	0.43	0.56	0.66	0.67	0.69	0.69	0.74	1.00					

DIT1		1	2	3	4	5	6	7	8	9	10	11	0.851	0.868
	DIT1	1.00												
	DIT2	0.39	1.00											
	DIT3	0.30	0.58	1.00										
	DIT4	0.21	0.42	0.44	1.00									
	DIT5	0.39	0.39	0.48	0.33	1.00								
	DIT6	0.17	0.48	0.50	0.47	0.39	1.00							
	DIT7	0.18	0.53	0.53	0.45	0.38	0.69	1.00						
	DIT8	0.20	0.38	0.37	0.52	0.33	0.58	0.62	1.00					
	DIT9	0.23	0.31	0.28	0.34	0.37	0.34	0.35	0.47	1.00				
	DIT10	0.34	0.21	0.25	0.29	0.27	0.26	0.27	0.36	0.65	1.00			
	DIT11	0.31	0.20	0.21	0.32	0.22	0.20	0.19	0.35	0.56	0.74	1.00		
DIT2		12	13	14	15	16	17						0.754	0.788
	DIT12	1.00												
	DIT13	0.41	1.00											
	DIT14	0.24	0.45	1.00										
	DIT15	0.49	0.45	0.27	1.00									
	DIT16	0.15	0.39	0.49	0.32	1.00								
	DIT17	0.18	0.42	0.43	0.38	0.73	1.00							
INDSN		1	2	3	4								0.707	0.690
	INDSN1	1.00												
	INDSN2	0.51	1.00											
	INDSN3	0.26	0.35	1.00										
	INDSN4	0.31	0.43	0.31	1.00									
INDRB		1	2	3	4								0.773	0.829
	INDRB1	1.00												
	INDRB2	0.63	1.00											
	INDRB3	0.38	0.54	1.00										
	INDRB4	0.53	0.61	0.59	1.00									
INDIR		1	2	3	4								0.799	0.842
	INDIR1	1.00												
	INDIR2	0.66	1.00											
	INDIR3	0.55	0.60	1.00										
	INDIR4	0.48	0.58	0.57	1.00									
INDITS		1	2	3	4								0.807	0.881
	INDITS1	1.00												
	INDITS2	0.76	1.00											
	INDITS3	0.59	0.66	1.00										
	INDITS4	0.58	0.67	0.64	1.00									

Internet Activities

Table 6.16: Internet Activities of the participants from Saudi Arabia and Malaysia

Internet Activities		Saudi Arabia		Malaysia	
		Frequency	%	Frequency	%
Email	Never	28	5.4	2	0.6
	Once or few times in my life	34	6.6	6	1.7
	Sometimes, but less than once a week	56	10.9	25	6.9
	At least once a week	102	19.8	94	25.9
	Almost everyday	295	57.3	236	65
Search Engines	Never	6	1.2	6	1.7
	Once or few times in my life	13	2.5	8	2.2
	Sometimes, but less than once a week	19	3.7	21	5.8
	At least once a week	76	14.8	74	20.4
	Almost everyday	401	77.9	254	70
Social Network	Never	96	18.6	7	1.9
	Once or few times in my life	70	13.6	7	1.9
	Sometimes, but less than once a week	135	26.2	22	6.1
	At least once a week	123	23.9	62	17.1
	Almost everyday	91	17.7	265	73
Newspaper	Never	79	15.3	11	3
	Once or few times in my life	85	16.5	25	6.9
	Sometimes, but less than once a week	121	23.5	64	17.6
	At least once a week	115	22.3	130	35.8
	Almost everyday	115	22.3	133	36.6
Instant Message	Never	48	9.3	13	3.6
	Once or few times in my life	40	7.8	13	3.6
	Sometimes, but less than once a week	41	8	55	15.2
	At least once a week	104	20.2	96	26.4
	Almost everyday	282	54.8	186	51.2
Online Game	Never	166	32.2	112	30.9
	Once or few times in my life	96	18.6	90	24.8
	Sometimes, but less than once a week	107	20.8	104	28.7
	At least once a week	86	16.7	34	9.4
	Almost everyday	60	11.7	23	6.3
Video Sharing	Never	33	6.4	33	9.1
	Once or few times in my life	31	6	49	13.5
	Sometimes, but less than once a week	83	16.1	88	24.2
	At least once a week	193	37.5	118	32.5
	Almost everyday	174	33.8	75	20.7
Live TV	Never	174	33.8	67	18.5
	Once or few times in my life	121	23.5	56	15.4
	Sometimes, but less than once	113	21.9	119	32.8

	a week				
	At least once a week	75	14.6	81	22.3
	Almost everyday	32	6.2	40	11
e-Commerce Website	Never	210	40.8	137	37.7
	Once or few times in my life	136	26.4	87	24
	Sometimes, but less than once a week	113	21.9	80	22
	At least once a week	40	7.8	44	12.1
	Almost everyday	16	3.1	15	4.1
Online Banking	Never	161	31.3	166	45.7
	Once or few times in my life	114	22.1	82	22.6
	Sometimes, but less than once a week	142	27.6	59	16.3
	At least once a week	68	13.2	42	11.6
	Almost everyday	30	5.8	14	3.9
e-Government website	Never	205	39.8	70	19.3
	Once or few times in my life	165	32	99	27.3
	Sometimes, but less than once a week	98	19	103	28.4
	At least once a week	25	4.9	58	16
	Almost everyday	22	4.3	33	9.1

Table 6.17: Internet Activities that reported to be used at least once or few times in their life

	Saudi Arabia	**Malaysia**
Internet Activities	**%**	**%**
Email	96.6	99.4
Search Engines	98.8	98.3
Social Network	81.4	98.1
Newspaper	84.7	97
Instant Message	90.7	96.4
Online Game	67.8	69.1
Video Sharing	93.6	90.9
Live TV	66.2	81.5
e-Commerce Website	59.2	62.3
Online Banking	68.7	54.3
e-Government website	60.2	80.7

Privacy Concerns 1

Table 6.18: Concern about submitting personal information via different Internet website

Concern about submitting personal information via		Saudi Arabia		Malaysia	
		Frequency	%	Frequency	%
Email	Disagree	160	31.1	20	5.5
	Neither agree nor disagree	150	29.1	51	14
	Agree	205	39.8	292	80
Search Engines	Disagree	191	37.1	57	15.7
	Neither agree nor disagree	148	28.7	124	34.2
	Agree	176	34.2	182	50.1
Social Network	Disagree	211	41	44	12.1
	Neither agree nor disagree	131	25.4	73	20.1
	Agree	173	33.6	246	67.8
Newspaper	Disagree	183	25.5	74	20.4
	Neither agree nor disagree	161	31.3	121	33.3
	Agree	171	33.2	168	46.3
Instant Message	Disagree	176	34.2	33	9.1
	Neither agree nor disagree	109	21.2	83	22.9
	Agree	230	44.7	247	68
Online Game	Disagree	221	42.9	128	35.3
	Neither agree nor disagree	130	25.2	114	31.4
	Agree	164	31.8	121	33.3
Video Sharing	Disagree	251	48.7	121	33.3
	Neither agree nor disagree	104	20.2	90	24.8
	Agree	160	31.1	152	41.9
Live TV	Disagree	226	43.9	93	25.6
	Neither agree nor disagree	131	25.4	112	30.9
	Agree	158	30.7	158	43.5
e-Commerce Website	Disagree	144	28	84	23.1
	Neither agree nor disagree	119	23.1	112	30.9
	Agree	252	48.9	167	46
Online Banking	Disagree	155	30.1	82	22.6
	Neither agree nor disagree	88	17.1	90	24.8
	Agree	272	52.8	191	52.6
e-Government website	Disagree	142	27.6	54	14.9
	Neither agree nor disagree	76	14.8	92	25.3
	Agree	297	57.7	217	59.8

Privacy Concerns 2

Table 6.19: Concern about submitting personal information via different Internet website

I am concerned that the information I submit on the Internet could be		Saudi Arabia		Malaysia	
		Frequency	%	Frequency	%
found by other	Disagree	97	18.8	21	5.8
	Neither agree nor disagree	65	12.6	43	11.8
	Agree	353	68.5	299	82.4
used by other	Disagree	100	19.4	35	9.7
	Neither agree nor disagree	34	6.6	42	11.6
	Agree	381	74	285	78.7
used in a way that I did not expected	Disagree	94	18.3	31	8.5
	Neither agree nor disagree	27	5.2	53	14.6
	Agree	394	76.5	278	76.6
used in a way that I did not comfortable with	Disagree	96	18.6	34	9.4
	Neither agree nor disagree	51	9.9	45	12.4
	Agree	368	71.5	284	78.2
used in a way that I could threat my security	Disagree	90	17.5	30	8.3
	Neither agree nor disagree	56	10.9	41	11.3
	Agree	369	71.7	291	80.2
used in a way that could not invade my privacy	Disagree	88	17.1	31	8.5
	Neither agree nor disagree	39	7.6	42	11.6
	Agree	388	75.3	290	79.9
used in a way that I could create unexpected problems	Disagree	101	19.6	30	8.3
	Neither agree nor disagree	34	6.6	45	12.4
	Agree	380	73.8	287	79.1
misused	Disagree	88	17.1	41	11.3
	Neither agree nor disagree	38	7.4	60	16.5
	Agree	389	75.5	262	72.2

Internet Trust – Information Security

Table 6.20: Concern about submitting personal information via different Internet website

It is safe to exchange information with others using		Saudi Arabia		Malaysia	
		Frequency	**%**	**Frequency**	**%**
Email	Disagree	159	30.9	62	17.1
	Neither agree nor disagree	90	17.517.9	58	16
	Agree	266	51.7	243	66.9
Social Network	Disagree	274	53.2	129	35.5
	Neither agree nor disagree	127	24.7	114	31.4
	Agree	114	22.1	120	33.1
Newspaper	Disagree	258	50.1	113	31.1
	Neither agree nor disagree	141	27.4	149	41
	Agree	115	22.3	101	27.8
Instant Message	Disagree	202	39.2	104	28.7
	Neither agree nor disagree	118	22.9	98	27
	Agree	195	37.9	161	44.4
Online Game	Disagree	341	66.2	195	53.7
	Neither agree nor disagree	106	20.6	129	35.5
	Agree	68	13.2	39	10.7
Video Sharing	Disagree	388	75.3	205	56.5
	Neither agree nor disagree	75	14.6	111	30.6
	Agree	52	10.1	47	12.9

Internet Trust – Professional Handling

Table 6.21: Concern about submitting personal information via different Internet website

I believe that my personal information are handled in a professional way when I submitted by		Saudi Arabia		Malaysia	
		Frequency	%	Frequency	%
Email	Disagree	123	23.9	34	9.4
	Neither agree nor disagree	121	23.5	58	16
	Agree	271	52.6	271	74.7
Search Engines	Disagree	198	38.4	104	28.7
	Neither agree nor disagree	154	29.9	149	41
	Agree	163	31.7	110	30.3
Social Network	Disagree	215	41.7	103	28.4
	Neither agree nor disagree	160	31.1	125	34.4
	Agree	140	27.2	135	37.2
Newspaper	Disagree	184	35.7	79	21.8
	Neither agree nor disagree	178	34.6	150	41.3
	Agree	153	29.7	134	36.9
Instant Message	Disagree	196	38.1	82	22.6
	Neither agree nor disagree	144	28	128	35.3
	Agree	175	34	153	42.1
Online Game	Disagree	263	51.1	179	49.3
	Neither agree nor disagree	173	33.6	140	38.6
	Agree	79	15.3	44	12.1
Video Sharing	Disagree	283	55	176	48.5
	Neither agree nor disagree	141	27.4	134	36.9
	Agree	91	17.7	53	14.6
Live TV	Disagree	245	47.6	130	35.8
	Neither agree nor disagree	154	29.9	149	41
	Agree	115	22.3	84	23.1
e-Commerce Website	Disagree	156	30.3	97	26.7
	Neither agree nor disagree	146	28.3	129	35.5
	Agree	213	41.4	137	37.7
Online Banking	Disagree	102	19.8	91	25.1
	Neither agree nor disagree	89	17.3	83	22.9
	Agree	324	62.9	189	52.1
e-Government website	Disagree	96	18.6	65	17.9
	Neither agree nor disagree	92	17.9	75	20.7
	Agree	327	63.5	223	61.4

Keeping my personal Information

Table 6.22: Keeping my personal Information

Keeping my personal Information is very important according to		Saudi Arabia		Malaysia	
		Frequency	%	Frequency	%
my family and friends	Disagree	96	1836	8	2.2
	Neither agree nor disagree	77	15	27	7.4
	Agree	342	66.4	327	90.1
my religion	Disagree	72	14	12	3.3
	Neither agree nor disagree	80	15.5	94	25.9
	Agree	363	70.5	257	70.8
Internet regulation in my country	Disagree	105	20.4	23	6.3
	Neither agree nor disagree	154	29.9	123	33.9
	Agree	256	49.7	217	59.8
my IT skill	Disagree	78	15.1	22	61
	Neither agree nor disagree	149	28.9	110	30.3
	Agree	288	55.9	231	63.6

Care about my privacy

Table 6.23: Care about my privacy

I should care about my privacy according to		Saudi Arabia		Malaysia	
		Frequency	%	Frequency	%
my family and friends	Disagree	88	17.1	8	1.7
	Neither agree nor disagree	82	1539	31	9.4
	Agree	345	67	324	89
my religion	Disagree	58	11.3	15	4.1
	Neither agree nor disagree	72	14	81	22.3
	Agree	385	74.8	267	73.6
Internet regulation in my country	Disagree	85	16.5	29	8
	Neither agree nor disagree	141	27.4	111	30.6
	Agree	289	56.1	222	61.2
my IT skill	Disagree	71	13.8	27	7.4
	Neither agree nor disagree	136	26.4	100	27.5
	Agree	308	59.8	236	65

Care about others privacy

Table 6.24: Care about others privacy

I should care about others privacy according to		Saudi Arabia		Malaysia	
		Frequency	%	Frequency	%
my family and friends	Disagree	72	14	6	1.7
	Neither agree nor disagree	88	17.1	34	9.4
	Agree	355	68.9	323	89
my religion	Disagree	71	13.8	13	3.6
	Neither agree nor disagree	80	15.5	59	16.3
	Agree	364	70.7	291	80.2
Internet regulation in my country	Disagree	77	15	22	6.1
	Neither agree nor disagree	131	25.4	95	26.2
	Agree	307	59.6	246	67.8
my IT skill	Disagree	67	13.8	29	8
	Neither agree nor disagree	148	26.4	99	27.3
	Agree	300	58.3	235	64.7

Careful when revealing personal information

Table 6.25: Careful when revealing personal information

I should be careful when revealing personal information according to		Saudi Arabia		Malaysia	
		Frequency	%	Frequency	%
my family and friends	Disagree	104	20.2	12	3.3
	Neither agree nor disagree	103	20	38	10.5
	Agree	308	59.8	313	86.2
my religion	Disagree	71	13.8	15	4.1
	Neither agree nor disagree	80	15.5	77	21.2
	Agree	364	70.7	271	74.7
Internet regulation in my country	Disagree	91	17.7	15	4.1
	Neither agree nor disagree	144	28	110	30.3
	Agree	279	54.2	238	65.6
my IT skill	Disagree	82	15.9	22	6.1
	Neither agree nor disagree	154	29.9	106	29.2
	Agree	279	54.2	235	64.7